



STIC Search Report

EIC 3600

STIC Database Tracking Number: 169476

TO: Pierre Elisca
Location: Knox 5A55
Art Unit : 3621
Case Serial Number: 09/710776

From: Janice Burns
Location: EIC 3600
Knox 4B71
Phone: 23518
Janice.Burns@uspto.gov

Search Notes

Dear Examiner Elisca

Please review the following results.

If you have any questions or would like a refocused, just let me know.

Janice Burns, MLS
ASRC Aerospace Corporation
US Patent & Trademark Office
Scientific & Technical Information Center
Electronic Information Center 3600
571-272-3518
571-273-0046 (fax)
Janice.Burns@uspto.gov





705/75

(95)

STIC EIC 3600 Search Request Form

169476

Today's Date:

10/25/05

What date would you like to use to limit the search? For 705 list subclass

Name ELISA PIERRE E.AU 3621 Examiner # 74461Room # 5A55 Phone 26706Serial # 09/710,776

Format for Search Results (Circle One):

PAPER DISK EMAIL

Where have you searched so far?

USP DWPI EPO JPO ACM IBM TDB

IEEE INSPEC SPI Other _____

Is this a "Fast & Focused" Search Request? (Circle One) YES NO

A "Fast & Focused" Search is completed in 2-3 hours (maximum). The search must be on a very specific topic and meet certain criteria. The criteria are posted in EIC3600 and on the EIC3600 NPL Web Page at <http://ptoweb/patents/stic/stic-tc3600.htm>.

What is the topic, novelty, motivation, utility, or other specific details defining the desired focus of this search? Please include the concepts, synonyms, keywords, acronyms, definitions, strategies, and anything else that helps to describe the topic. Please attach a copy of the abstract, background, brief summary, pertinent claims and any citations of relevant art you have found.

ABC Attached
claim 1

Oh Fresh.

SPEC 21

STIC Searcher _____ Phone _____

Date picked up _____ Date Completed _____



Set	Items	Description
S1	4	AU=(CANDELLA, G? OR CANDELLA G?)
S2	3	AU=(NOHAVEC, I? OR NOHAVEC I?)
S3	34	AU=(SCRUGGS, M? OR SCRUGGS M?)
S4	3	S1 AND S2 AND S3

File 350:Derwent WPIX 1963-2005/UD,UM &UP=200568
(c) 2005 Thomson Derwent

File 344:Chinese Patents Abs Aug 1985-2005/May
(c) 2005 European Patent Office

File 347:JAPIO Nov 1976-2005/Jun(Updated 051004)
(c) 2005 JPO & JAPIO

File 348:EUROPEAN PATENTS 1978-2005/Oct W03
(c) 2005 European Patent Office

File 349:PCT FULLTEXT 1979-2005/UB=20051020,UT=20051013
(c) 2005 WIPO/Univentio

4/5/1 (Item 1 from file: 350)
 DIALOG(R)File 350:Derwent WPIX
 (c) 2005 Thomson Derwent. All rts. reserv.

014122850 **Image available**

WPI Acc No: 2001-607062/200169

XRPX Acc No: N01-453166

Fraud detection method e.g. for non personal transactions such as when shipping address is different to billing address, involves transmitting the purchaser's data, including ship-to address for the transaction, to fraud- detection system

Patent Assignee: FRAUD-CHECK.COM INC (FRAU-N); SCRUGGS M L (SCRU-I)

Inventor: CANDELLA G J ; NOHAVEC I H ; SCRUGGS M L

Number of Countries: 093 Number of Patents: 004

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 200135301	A1	20010517	WO 2000US30981	A	20001109	200169 B
AU 200117617	A	20010606	AU 200117617	A	20001109	200169
GB 2379758	A	20030319	WO 2000US30981	A	20001109	200321
			GB 200210620	A	20020509	
AU 777445	B2	20041014	AU 200117617	A	20001109	200501

Priority Applications (No Type Date): US 99164444 P 19991109

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes

WO 200135301 A1 E 36 G06F-017/60

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW

Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW

AU 200117617	A	G06F-017/60	Based on patent WO 200135301
GB 2379758	A	G06F-017/60	Based on patent WO 200135301
AU 777445	B2	G06F-017/60	Previous Publ. patent AU 200117617 Based on patent WO 200135301

Abstract (Basic): WO 200135301 A1

NOVELTY - The method involves transmitting the purchaser's data, including a ship-to address for the transaction, to a fraud-detection system (100). The purchaser's data is processed to determine whether the transaction is potentially fraudulent (102, 104, 106) and the relative risks of fraudulent activity associated with the transaction is returned.

DETAILED DESCRIPTION - A check is made determine whether the purchaser's ship-to address exists and the purchaser's ship-to address against a historical database to determine whether a prior history of fraud exists. The purchaser's ship-to address is checked against an historical database to determine whether a pattern of fraudulent activity exists for the ship-to address and against a modeling engine to determine whether elements exist in the demographic data which correlate with fraudulent trends.

USE - For detecting fraud in non personal transactions.

ADVANTAGE - Reduces risk and losses.

DESCRIPTION OF DRAWING(S) - The figure shows a schematic drawing of the method of detecting fraud in accordance with the invention.

Fraud-detection system (100)

Transaction is potentially fraudulent (102, 104, 106)

pp; 36 DwgNo 2/8

Title Terms: FRAUD; DETECT; METHOD; NON; PERSON; TRANSACTION; SHIPPING; ADDRESS; BILL; ADDRESS; TRANSMIT; PURCHASE; DATA; SHIP; ADDRESS;

TRANSACTION; FRAUD; DETECT; SYSTEM
Derwent Class: T01; W01
International Patent Class (Main): G06F-017/60
File Segment: EPI

4/5/2 (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2005 European Patent Office. All rts. reserv.

01302010

METHOD AND SYSTEM FOR DETECTING FRAUD IN NON-PERSONAL TRANSACTIONS
PROCEDE ET SYSTEME DE DETECTION DES FRAUDES DANS DES TRANSACTIONS NON
PERSONNELLES

PATENT ASSIGNEE:

Fraud-Check. Com, Inc., (3331110), 70 West Red Oak Lane, White Plains, NY
10604, (US), (Applicant designated States: all)
Scruggs, Michael L., (3942940), 2020 Long Tail Trail, Argyle, TX
76226-4500, (US), (Applicant designated States: all)

INVENTOR:

CANDELLA, George, J. , 348A Heritage Hills, Somers, NY 10589, (US)
NOHAVEC, Irene, H. , 48 De Motte Avenue, Clifton, NJ 07011, (US)
SCRUGGS, Michael, L. , 2020 Longtail Trail, Argyle, TX 76226-4500, (US)

PATENT (CC, No, Kind, Date):

WO 2001035301 010517

APPLICATION (CC, No, Date): EP 2000980342 001109; WO 2000US30981 001109

PRIORITY (CC, No, Date): US 164444 P 991109

DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI;
LU; MC; NL; PT

EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI

INTERNATIONAL PATENT CLASS: G06F-017/60

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application: 010711 A1 International application. (Art. 158(1))

Application: 010711 A1 International application entering European
phase

Application: 030102 A1 International application. (Art. 158(1))

Appl Changed: 030102 A1 International application not entering European
phase

Withdrawal: 030102 A1 Date application deemed withdrawn: 20020611

LANGUAGE (Publication,Procedural,Application): English; English; English

4/5/3 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2005 WIPO/Univentio. All rts. reserv.

00801780 **Image available**

METHOD AND SYSTEM FOR DETECTING FRAUD IN NON-PERSONAL TRANSACTIONS
PROCEDE ET SYSTEME DE DETECTION DES FRAUDES DANS DES TRANSACTIONS NON
PERSONNELLES

Patent Applicant/Assignee:

FRAUD-CHECK COM INC, 70 West Red Oak Lane, White Plains, NY 10604, US, US
(Residence), US (Nationality)

Inventor(s):

CANDELLA George J , 348A Heritage Hills, Somers, NY 10589, US,
NOHAVEC Irene H , 48 De Motte Avenue, Clifton, NJ 07011, US,
SCRUGGS Michael L , 2020 Longtail Trail, Argyle, TX 76226-4500, US

Legal Representative:

DE ROSA Kenneth R (agent), Wolf, Block, Schorr and Solis-Cohen LLP, 22nd
floor, 1650 Arch Street, Philadelphia, PA 19103-2097, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200135301 A1 20010517 (WO 0135301)
Application: WO 2000US30981 20001109 (PCT/WO US0030981)
Priority Application: US 99164444 19991109

Designated States:

(Protection type is "patent" unless otherwise stated - for applications prior to 2004)

AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE
ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT
LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM
TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM

Main International Patent Class: G06F-017/60

Publication Language: English

Filing Language: English

Fulltext Availability:

Detailed Description

Claims

Fulltext Word Count: 6925

English Abstract

A method and system is disclosed for detecting fraud (100) in non-personal transactions. The method and system comprise transmitting the purchaser's data, includes a ship-to address for the transaction, to a fraud-detection system (100); processing the purchaser's data to determine whether the transaction is potentially fraudulent (102, 104, 106); and returning the relative risks of fraudulent activity associated with the transaction. The method and system may include any of the following additional steps: checking to determine whether the purchaser's ship-to address (122) exists, checking the purchaser's ship-to address against a historical database to determine whether a prior history of fraud (172) exists, checking the purchaser's ship-to address against an historical database to determine whether a pattern of fraudulent activity (126) exists for the ship-to address; and checking the purchaser's ship-to address against a modeling engine (128) to determine whether elements exist in the demographic data which correlate with fraudulent trends. In addition, a score (130) may be calculated based at least in part upon the likelihood that the transaction is fraudulent.

French Abstract

L'invention concerne un procede et un systeme de detection des fraudes (100) dans des transactions non personnelles. Le procede et le systeme consistent a transmettre les donnees de l'acheteur, comprenant une adresse d'expedition, a un systeme de detection des fraudes (100); a traiter les donnees de l'acheteur afin de determiner si la transaction est potentiellement frauduleuse (102, 104, 106); et a renvoyer les risques relatifs d'activite frauduleuse associes a la transaction. Le procede et le systeme peuvent comprendre les etapes suivantes consistant a : verifier si l'adresse d'expedition de l'acheteur (122) existe, verifier l'adresse d'expedition de l'acheteur dans une base de donnees chronologique pour determiner s'il existe un antecedent de fraude (172); verifier l'adresse d'expedition de l'acheteur dans une base de donnees chronologique pour determiner s'il existe un schema d'activite frauduleuse (126) pour l'adresse d'expedition donnee; et verifier l'adresse d'expedition de l'acheteur dans un moteur de modelisation (128) pour determiner s'il existe des elements dans les donnees demographiques qui sont en correlation avec des tendances a la fraude. De plus, un indice (130) peut etre calcule sur la base, au moins en partie, de la

probabilite que la transaction soit frauduleuse.

Legal Status (Type, Date, Text)

Publication 20010517 A1 With international search report.

Publication 20010517 A1 Before the expiration of the time limit for
amending the claims and to be republished in the
event of the receipt of amendments.

Examination 20010927 Request for preliminary examination prior to end of
19th month from priority date

Set	Items	Description
S1	4	AU=(CANDELLA, G? OR CANDELLA G?)
S2	3	AU=(NOHAVEC, I? OR NOHAVEC I?)
S3	34	AU=(SCRUGGS, M? OR SCRUGGS M?)
S4	3	S1 AND S2 AND S3
S5	35	S1 OR S2 OR S3
S6	32	S5 NOT S4
S7	1	S6 AND IC=G06F-017/60
S8	1	S6 AND IC=G06F?

File 350:Derwent WPIX 1963-2005/UD,UM &UP=200568
(c) 2005 Thomson Derwent

File 344:Chinese Patents Abs Aug 1985-2005/May
(c) 2005 European Patent Office

File 347:JAPIO Nov 1976-2005/Jun(Updated 051004)
(c) 2005 JPO & JAPIO

File 348:EUROPEAN PATENTS 1978-2005/Oct W03
(c) 2005 European Patent Office

File 349:PCT FULLTEXT 1979-2005/UB=20051020,UT=20051013
(c) 2005 WIPO/Univentio

8/5/1 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2005 Thomson Derwent. All rts. reserv.

016826309 **Image available**
WPI Acc No: 2005-150591/200516
XRPX Acc No: N05-126960

**Identity theft detecting method for e.g. personal commerce transaction,
involves checking external address against respective known fraud and
good address table databases to find if address is fraudulent and
potentially fraudulent**

Patent Assignee: CANDELLA G J (CAND-I); CASS J (CASS-I); KELLAND K (KELL-I)
Inventor: **CANDELLA G J** ; CASS J; KELLAND K
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 20050021476	A1	20050127	US 2001303490	P	20010706	200516 B
			US 2002384061	P	20020528	
			US 2002189898	A	20020703	

Priority Applications (No Type Date): US 2002189898 A 20020703; US
2001303490 P 20010706; US 2002384061 P 20020528

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20050021476	A1		14	G06F-017/60	Provisional application US 2001303490

Provisional application US 2002384061

Abstract (Basic): US 20050021476 A1

NOVELTY - The method involves comparing an address to an external address database to find if the address is potentially fraudulent. The address is checked against known fraud and good address table databases to find if the address is fraudulent and potentially fraudulent; respectively. One database is queried for available incidental data of the address. A user is asked a question based upon the incidental data to verify user identity.

USE - Used for detecting identity theft in non-personal and personal commerce transaction.

ADVANTAGE - The address is checked against known fraud and good address table databases to find if the address is fraudulent and potentially fraudulent, respectively, thus reducing risk of loss and threats to safety associated with it.

DESCRIPTION OF DRAWING(S) - The drawing shows a schematic view of a portion of a method and system for detecting identity theft.

pp; 14 DwgNo 2A/5

Title Terms: IDENTIFY; THEFT; DETECT; METHOD; PERSON; TRANSACTION; CHECK;
EXTERNAL; ADDRESS; RESPECTIVE; FRAUD; ADDRESS; TABLE; FINDER; ADDRESS;
FRAUD; POTENTIALLY; FRAUD

Derwent Class: T01; T05; W02

International Patent Class (Main): **G06F-017/60**

File Segment: EPI

Set	Items	Description
S1	1	AU=(CANDELLA, G? OR CANDELLA G?)
S2	0	AU=(NOHAVEC, I? OR NOHAVEC I?)
S3	4	AU=(SCRUGGS, M? OR SCRUGGS M?)
S4	0	S1 AND S3
S5	5	S1 OR S3
S6	5	RD (unique items)
File 2:	INSPEC 1898-2005/Oct W3	(c) 2005 Institution of Electrical Engineers
File 35:	Dissertation Abs Online 1861-2005/Oct	(c) 2005 ProQuest Info&Learning
File 65:	Inside Conferences 1993-2005/Oct W4	(c) 2005 BLDSC all rts. reserv.
File 99:	Wilson Appl. Sci & Tech Abs 1983-2005/Sep	(c) 2005 The HW Wilson Co.
File 474:	New York Times Abs 1969-2005/Oct 26	(c) 2005 The New York Times
File 475:	Wall Street Journal Abs 1973-2005/Oct 26	(c) 2005 The New York Times
File 583:	Gale Group Globalbase(TM) 1986-2002/Dec 13	(c) 2002 The Gale Group
File 15:	ABI/Inform(R) 1971-2005/Oct 27	(c) 2005 ProQuest Info&Learning
File 20:	Dialog Global Reporter 1997-2005/Oct 27	(c) 2005 Dialog
File 610:	Business Wire 1999-2005/Oct 27	(c) 2005 Business Wire.
File 810:	Business Wire 1986-1999/Feb 28	(c) 1999 Business Wire
File 476:	Financial Times Fulltext 1982-2005/Oct 27	(c) 2005 Financial Times Ltd
File 613:	PR Newswire 1999-2005/Oct 27	(c) 2005 PR Newswire Association Inc
File 813:	PR Newswire 1987-1999/Apr 30	(c) 1999 PR Newswire Association Inc
File 634:	San Jose Mercury Jun 1985-2005/Oct 26	(c) 2005 San Jose Mercury News
File 624:	McGraw-Hill Publications 1985-2005/Oct 27	(c) 2005 McGraw-Hill Co. Inc
File 9:	Business & Industry(R) Jul/1994-2005/Oct 26	(c) 2005 The Gale Group
File 275:	Gale Group Computer DB(TM) 1983-2005/Oct 26	(c) 2005 The Gale Group
File 621:	Gale Group New Prod. Annou. (R) 1985-2005/Oct 27	(c) 2005 The Gale Group
File 636:	Gale Group Newsletter DB(TM) 1987-2005/Oct 26	(c) 2005 The Gale Group
File 16:	Gale Group PROMT(R) 1990-2005/Oct 26	(c) 2005 The Gale Group
File 160:	Gale Group PROMT(R) 1972-1989	(c) 1999 The Gale Group
File 148:	Gale Group Trade & Industry DB 1976-2005/Oct 27	(c) 2005 The Gale Group
File 256:	TecInfoSource 82-2005/Jan	(c) 2005 Info.Sources Inc

6/5/1 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC
(c) 2005 Institution of Electrical Engineers. All rts. reserv.

04891868 INSPEC Abstract Number: B91037381

Title: Casting and machining of devices of high temperature superconducting BSCCO (magnetic shields)

Author(s): Rayne, R.J.; Toth, L.E.; Bender, B.A.; Lawrence, S.H.; Miller, M.M.; Soulen, R.J., Jr.; **Candella, G.**

Author Affiliation: Naval Res. Lab., Washington, DC, USA

Journal: Journal of Materials Research vol.6, no.3 p.467-72

Publication Date: March 1991 Country of Publication: USA

CODEN: JMREEE ISSN: 0884-2914

Language: English Document Type: Journal Paper (JP)

Treatment: Practical (P); Experimental (X)

Abstract: Magnetic shields for SQUID applications were successfully fabricated using high T/sub c/ superconducting Bi-Sr-Ca-Cu-O (BSCCO). In order to produce shields with adequate superconducting properties and close dimensional control, it was necessary to develop several new processing techniques. Shields were produced by casting liquid BSCCO into molds, heat treating, and machining. A series of BSCCO alloys with different compositions were cast from the molten state into metal molds and subsequently heat treated to render the castings superconducting. The heat-treating cycles were studied with the aid of thermogravimetric analysis (TGA), differential thermal analysis (DTA), and dilatometer measurements. The phases and microstructures after various heat-treating cycles were monitored by X-ray diffraction (XRD), optical microscopy, and scanning electron microscopy (SEM). Superconducting properties were measured after various stages of heat treatment and machining. Prototype magnetic shields were machined from bulk castings and found to perform successfully. The most significant factor in shield quality was the nominal composition of the shield, which was shown by transmission electron microscopy (TEM) to affect the grain boundary chemistry. (13 Refs)

Subfile: B

Descriptors: bismuth compounds; calcium compounds; casting; crystal microstructure; grain boundaries; heat treatment; high-temperature superconductors; magnetic shielding; optical microscopy; phase equilibrium; scanning electron microscope examination of materials; strontium compounds; thermal analysis; transmission electron microscope examination of materials; X-ray diffraction examination of materials

Identifiers: high temperature superconductors; SEM; magnetic shields; TGA; DTA; XRD; TEM; machining; devices; high temperature superconducting BSCCO; SQUID applications; close dimensional control; casting; molds; heat treating; heat-treating cycles; thermogravimetric analysis; differential thermal analysis; dilatometer measurements; phases; microstructures; X-ray diffraction; optical microscopy; scanning electron microscopy; shield quality; nominal composition; transmission electron microscopy; grain boundary chemistry; Bi-Sr-Ca-Cu-O

Class Codes: B0540 (Ceramics and refractories); B3240G (Other superconducting material applications and devices); B5230 (Electromagnetic compatibility and interference)

Chemical Indexing:

BiSrCaCuO ss - Bi ss - Ca ss - Cu ss - Sr ss - O ss (Elements - 5)

6/5/2 (Item 1 from file: 35)
DIALOG(R)File 35:Dissertation Abs Online
(c) 2005 ProQuest Info&Learning. All rts. reserv.

578622 ORDER NO: AAD76-29482

DETERMINATION OF THE VERTICAL DISTRIBUTION OF OZONE WITH SIMULTANEOUS

UMKEHR-OZONESONDE OBSERVATIONS OVER TALLAHASSEE, FLORIDA.

Author: SCRUGGS, MARK ALAN
Degree: PH.D.
Year: 1976
Corporate Source/Institution: THE FLORIDA STATE UNIVERSITY (0071)
Source: VOLUME 37/07-B OF DISSERTATION ABSTRACTS INTERNATIONAL.
PAGE 3478. 117 PAGES
Descriptors: PHYSICS, ATMOSPHERIC SCIENCE
Descriptor Codes: 0608

6/5/3 (Item 2 from file: 35)

DIALOG(R)File 35:Dissertation Abs Online
(c) 2005 ProQuest Info&Learning. All rts. reserv.

222314 ORDER NO: AAD59-05059

CRITERIA FOR DETERMINING EFFECTIVENESS OF HOMEMAKING TEACHERS

Author: SCRUGGS, MARY MARGUERITE
Degree: PH.D.
Year: 1959
Corporate Source/Institution: IOWA STATE UNIVERSITY (0097)
Source: VOLUME 20/06 OF DISSERTATION ABSTRACTS INTERNATIONAL.
PAGE 2269. 222 PAGES
Descriptors: HOME ECONOMICS
Descriptor Codes: 0386

6/5/4 (Item 1 from file: 65)

DIALOG(R)File 65:Inside Conferences
(c) 2005 BLDSC all rts. reserv. All rts. reserv.

04818253 INSIDE CONFERENCE ITEM ID: CN050269498

Reduction of Microbial Loads in Channel Catfish Processing Operations by Use of High-Pressure Sprays and Various Additives

Silva, P. L.; Silva, J. L.; Wang, C.; Scruggs, M. L.
CONFERENCE: Catfish processors-Workshop
BULLETIN-MISSISSIPPI AGRICULTURAL AND FORESTRY EXPERIMENT STATION , 2003;
(NO) 1121 P: 34-34
MAFES, 2003
LANGUAGE: English DOCUMENT TYPE: Conference Papers 1996 (1996) (1996)

BRITISH LIBRARY ITEM LOCATION: 2617.880000
DESCRIPTORS: catfish processors

6/5/5 (Item 1 from file: 148)

DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2005 The Gale Group. All rts. reserv.
>>>Accession number 7261697 is unavailable

Set	Items	Description
S1	5909680	DETECT??? OR CALCULAT? OR DETERMIN? OR COMPUT??? OR FIGURE- ??? OR ESTIMAT? OR GAUG?
S2	1437753	POTENTIAL? OR LIKELIHOOD OR RELATIVE OR POSSIBL? OR PROBAB- LE OR PROBABILITY OR LIKELY
S3	32701	FRAUD? OR DECEPTION? OR THEFT OR THIEV? OR LARCENY OR STEA- L? OR ROBBERY OR CHEAT? OR SWINDL? OR DISHONEST
S4	1075462	CHECK??? OR COMPAR??? OR VERIFY? OR VERIFI? OR CONFIRM??? - OR VALIDAT? OR AFFIRM? OR CORROBORAT? OR AUTHENTICAT?
S5	352885	(PURCHASER? OR BUYER? OR SHOPPER? OR CONSUMER? OR CUSTOMER? OR USER?)(1W)(DATA OR INFO OR INFORMATION) OR SHIP()TO OR SH- IPPING OR BILL()TO OR ADDRESS? OR AREA()CODE? OR PHONE()NUMBE- R? OR ZIP OR CRITERIA
S6	120975	RISK OR RISKS OR CHANCE OR SCORE
S7	14734	S1 AND S3
S8	1136	S7 AND S2
S9	58235	S4 AND S5
S10	32	S8 AND S9
S11	5	S10 AND S6
S12	4	S11 AND IC=G06F?

File 350:Derwent WPIX 1963-2005/UD,UM &UP=200568

(c) 2005 Thomson Derwent

File 344:Chinese Patents Abs Aug 1985-2005/May

(c) 2005 European Patent Office

File 347:JAPIO Nov 1976-2005/Jun(Updated 051004)

(c) 2005 JPO & JAPIO

12/5/1 (Item 1 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2005 Thomson Derwent. All rts. reserv.

016826309 **Image available**

WPI Acc No: 2005-150591/200516

XRPX Acc No: N05-126960

Identity theft detecting method for e.g. personal commerce transaction, involves checking external address against respective known fraud and good address table databases to find if address is fraudulent and potentially fraudulent

Patent Assignee: CANDELLA G J (CAND-I); CASS J (CASS-I); KELLAND K (KELL-I)

Inventor: CANDELLA G J; CASS J; KELLAND K

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 20050021476	A1	20050127	US 2001303490	P	20010706	200516 B
			US 2002384061	P	20020528	
			US 2002189898	A	20020703	

Priority Applications (No Type Date): US 2002189898 A 20020703; US

2001303490 P 20010706; US 2002384061 P 20020528

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20050021476	A1		14	G06F-017/60	Provisional application US 2001303490

Provisional application US 2002384061

Abstract (Basic): US 20050021476 A1

NOVELTY - The method involves **comparing** an **address** to an external **address** database to find if the **address** is **potentially fraudulent**. The **address** is **checked** against known **fraud** and good **address** table databases to find if the **address** is **fraudulent** and **potentially fraudulent**, respectively. One database is queried for available incidental data of the **address**. A user is asked a question based upon the incidental data to **verify** user identity.

USE - Used for **detecting** identity **theft** in non-personal and personal commerce transaction.

ADVANTAGE - The **address** is **checked** against known **fraud** and good **address** table databases to find if the **address** is **fraudulent** and **potentially fraudulent**, respectively, thus reducing **risk** of loss and threats to safety associated with it.

DESCRIPTION OF DRAWING(S) - The drawing shows a schematic view of a portion of a method and system for **detecting** identity **theft**.

pp; 14 DwgNo 2A/5

Title Terms: IDENTIFY; **THEFT**; **DETECT**; METHOD; PERSON; TRANSACTION;

CHECK; EXTERNAL; **ADDRESS**; RESPECTIVE; **FRAUD**; **ADDRESS**; TABLE;

FINDER; **ADDRESS**; **FRAUD**; **POTENTIALLY**; **FRAUD**

Derwent Class: T01; T05; W02

International Patent Class (Main): G06F-017/60

File Segment: EPI

12/5/2 (Item 2 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2005 Thomson Derwent. All rts. reserv.

014196823 **Image available**

WPI Acc No: 2002-017520/200202

XRPX Acc No: N02-014008

Method of detecting and evaluating fraud suspects by calculating a value for each suspect based on monetary transaction information and a number of different criteria and applying criteria weights to the values to produce a score

Patent Assignee: STERLING COMMERCE INC (STER-N); STERLING COMMERCE NORTHERN AMERICA INC (STER-N); VECTORSGI INC (VECT-N)

Inventor: CROOK T J; HOWELL J W; NIGRINI M J

Number of Countries: 096 Number of Patents: 004

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 200177960	A2	20011018	WO 2001US11281	A	20010406	200202 B
AU 200151403	A	20011023	AU 200151403	A	20010406	200213
EP 1334448	A2	20030813	EP 2001924780	A	20010406	200355
			WO 2001US11281	A	20010406	
JP 2004502994	W	20040129	JP 2001575335	A	20010406	200413
			WO 2001US11281	A	20010406	

Priority Applications (No Type Date): US 2000545046 A 20000407

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes

WO 200177960 A2 E 37 G06F-017/60

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW

Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW

AU 200151403 A Based on patent WO 200177960

EP 1334448 A2 E G06F-017/60 Based on patent WO 200177960

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR

JP 2004502994 W 58 G06F-017/60 Based on patent WO 200177960

Abstract (Basic): WO 200177960 A2

NOVELTY - Monetary transaction data associated with a **fraud** is received for each suspect and for each suspect a value is **calculated** for several parameters (22) associated with the **fraud** based on the monetary transaction data (46). **Criteria** weights are applied to the values for each suspect to generate a **score** indicative of the **likelihood of fraud**.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for

(a) a system for evaluating **fraud** suspects using a **computer** program.

(b) a method of **detecting fraud** at a financial institution.

(c) a system for **detecting fraud** at a financial institution using a **computer** program.

USE - **Detecting** and evaluating **fraud** suspects, e.g. in a **check** kiting scheme.

ADVANTAGE - Evaluation is based on a statistical analysis of a number of important **criteria** and provides an effective prioritization of suspects.

DESCRIPTION OF DRAWING(S) - The block diagram represents a system for identifying and evaluating **fraud** suspects.

Parameter files (22)

Transaction files (46)

pp; 37 DwgNo 1/4

Title Terms: METHOD; **DETECT**; **EVALUATE**; **FRAUD**; **CALCULATE**; **VALUE**;

SUSPECT; **BASED**; **MONEY**; **TRANSACTION**; **INFORMATION**; **NUMBER**; **CRITERIA**;

APPLY; **CRITERIA**; **WEIGHT**; **VALUE**; **PRODUCE**; **SCORE**

Derwent Class: T01; T05

International Patent Class (Main): **G06F-017/60**
 International Patent Class (Additional): G07F-007/08
 File Segment: EPI

12/5/3 (Item 3 from file: 350)
 DIALOG(R)File 350:Derwent WPIX
 (c) 2005 Thomson Derwent. All rts. reserv.

014122850 **Image available**
 WPI Acc No: 2001-607062/200169
 XRPX Acc No: N01-453166

Fraud detection method e.g. for non personal transactions such as when shipping address is different to billing address , involves transmitting the purchaser 's data , including ship - to address for the transaction, to fraud - detection system

Patent Assignee: FRAUD-CHECK.COM INC (FRAU-N); SCRUGGS M L (SCRU-I)

Inventor: CANDELLA G J; NOHAVEC I H; SCRUGGS M L

Number of Countries: 093 Number of Patents: 004

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 200135301	A1	20010517	WO 2000US30981	A	20001109	200169 B
AU 200117617	A	20010606	AU 200117617	A	20001109	200169
GB 2379758	A	20030319	WO 2000US30981	A	20001109	200321
			GB 200210620	A	20020509	
AU 777445	B2	20041014	AU 200117617	A	20001109	200501

Priority Applications (No Type Date): US 99164444 P 19991109

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes

WO 200135301 A1 E 36 G06F-017/60

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW

Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW

AU 200117617	A	G06F-017/60	Based on patent WO 200135301
GB 2379758	A	G06F-017/60	Based on patent WO 200135301
AU 777445	B2	G06F-017/60	Previous Publ. patent AU 200117617 Based on patent WO 200135301

Abstract (Basic): WO 200135301 A1

NOVELTY - The method involves transmitting the **purchaser 's data** , including a **ship - to address** for the transaction, to a **fraud - detection** system (100). The **purchaser 's data** is processed to **determine** whether the transaction is **potentially fraudulent** (102, 104, 106) and the **relative risks** of **fraudulent** activity associated with the transaction is returned.

DETAILED DESCRIPTION - A **check** is made **determine** whether the purchaser's **ship - to address** exists and the purchaser's **ship - to address** against a historical database to **determine** whether a prior history of **fraud** exists. The purchaser's **ship - to address** is **checked** against an historical database to **determine** whether a pattern of **fraudulent** activity exists for the **ship - to address** and against a modeling engine to **determine** whether elements exist in the demographic data which correlate with **fraudulent** trends.

USE - For **detecting fraud** in non personal transactions.

ADVANTAGE - Reduces **risk** and losses.

DESCRIPTION OF DRAWING(S) - The **figure** shows a schematic drawing

of the method of **detecting fraud** in accordance with the invention.

Fraud - detection system (100)

Transaction is **potentially fraudulent** (102, 104, 106)

pp; 36 DwgNo 2/8

Title Terms: **FRAUD ; DETECT ; METHOD; NON; PERSON; TRANSACTION; SHIPPING ; ADDRESS ; BILL; ADDRESS ; TRANSMIT; PURCHASE; DATA; SHIP; ADDRESS ; TRANSACTION; FRAUD ; DETECT ; SYSTEM**

Derwent Class: T01; W01

International Patent Class (Main): **G06F-017/60**

File Segment: EPI

12/5/4 (Item 4 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2005 Thomson Derwent. All rts. reserv.

011099715 **Image available**

WPI Acc No: 1997-077640/199707

XRPX Acc No: N97-064400

Fraud detection system for medical and banking industries - includes risk analysis processor comparing entity scores derived from analysis criteria giving indication of fraudulent activity

Patent Assignee: FRAUDETECT LLC (FRAU-N)

Inventor: COFOD R K

Number of Countries: 069 Number of Patents: 002

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 9700483	A1	19970103	WO 96US10352	A	19960614	199707 B
AU 9662798	A	19970115	AU 9662798	A	19960614	199718

Priority Applications (No Type Date): US 95490984 A 19950615

Cited Patents: US 5253164; US 5359509; US 5557514

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes

WO 9700483 A1 E 46 G06F-015/00

Designated States (National): AL AM AT AU AZ BB BG BR BY CA CH CN CZ DE DK EE ES FI GB GE HU IS JP KE KG KP KR KZ LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TR TT UA UG UZ VN

Designated States (Regional): AT BE CH DE DK EA ES FI FR GB GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG

AU 9662798 A G06F-015/00 Based on patent WO 9700483

Abstract (Basic): WO 9700483 A

The **fraud detection** system includes a statistical analysis engine generating statistical values for the entity according to at least one of numerous analysis **criteria**. An entity criterion **score** generator weights and sums each of the statistical values to form an entity criterion **score** for each of the analysis **criteria**.

An entity **score** generator weights and sums each entity criterion **score** to form a first entity **score**. Memory stores the statistical

values, the entity criterion scores and the first entity **score**.

A **risk** analysis processor **compares** the first entity **score** to

a

predetermined threshold, where the result of the comparison indicates whether the entity is engaging in a **fraudulent** activity.

ADVANTAGE - Provides **fraud** pre-processor **detection** system.

Allows

analysis of large volumes of transaction data to **detect fraud** .
Prioritises clients most **likely** to be engaging in **fraudulent**
behaviour. Provides list of actions to take against **fraudulent**
entities for selection by human analyst. Provides monitoring
facility after actions taken.

Dwg.7/8

Title Terms: **FRAUD** ; **DETECT** ; SYSTEM; MEDICAL; BANK; INDUSTRIAL; **RISK** ;
ANALYSE; PROCESSOR; **COMPARE** ; ENTITY; **SCORE** ; DERIVATIVE; ANALYSE;
CRITERIA ; INDICATE; **FRAUD** ; ACTIVE

Derwent Class: T01

International Patent Class (Main): **G06F-015/00**

International Patent Class (Additional): **G06F-017/60** ; G06G-007/52

File Segment: EPI

Set	Items	Description
S1	25990	FRAUD? OR DECEPTION? OR THEFT OR THIEV? OR LARCENY OR STEA- L? OR ROBBERY OR CHEAT? OR SWINDL? OR DISHONEST?
S2	1640515	DETECT??? OR CALCULAT? OR DETERMIN? OR COMPUT??? OR FIGURE- ??? OR ESTIMAT? OR GAUG?
S3	1417395	POTENTIAL? OR LIKELIHOOD OR RELATIVE OR POSSIBL? OR PROBAB- LE OR PROBABILITY OR LIKELY
S4	867484	CHECK??? OR COMPAR??? OR VERIFY? OR VERIFI? OR CONFIRM??? - OR VALIDAT? OR AFFIRM? OR CORROBORAT? OR AUTHENTICAT?
S5	365661	(PURCHASER? OR BUYER? OR SHOPPER? OR CONSUMER? OR CUSTOMER? OR USER?)(1W)(DATA OR INFO OR INFORMATION) OR SHIP()TO OR SH- IPPING OR BILL()TO OR ADDRESS? OR AREA()CODE? OR PHONE()NUMBE- R? OR ZIP
S6	235089	RISK OR RISKS OR CHANCE OR SCORE
S7	5523	S1(10N)S2
S8	28477	S4(10N)S5
S9	163	S7(S)S8
S10	61	S9(S)S3
S11	27	S10(S)S6
S12	12	S11 AND IC=G06F-017/60

File 348:EUROPEAN PATENTS 1978-2005/Oct W03

(c) 2005 European Patent Office

File 349:PCT FULLTEXT 1979-2005/UB=20051020,UT=20051013

(c) 2005 WIPO/Univentio

12/3,K/1 (Item 1 from file: 348)
 DIALOG(R)File 348:EUROPEAN PATENTS
 (c) 2005 European Patent Office. All rts. reserv.

01930027

Secure transaction management**Verfahren und Vorrichtung zur gesicherten Transaktionsverwaltung****Procede et dispositif de gestion de transactions securisees****PATENT ASSIGNEE:**

Intertrust Technologies Corp., (2434323), 955 Stewart Drive, Sunnyvale,
 CA 94085, (US), (Applicant designated States: all)

INVENTOR:

Ginter, Karl L., 10404 43rd Avenue, Beltsville, MD 20705, (US)
 Spahn, Francis J., 2410 Edwards Avenue, El Cerrito, CA 94530, (US)
 Shear, Victor H., 5203 Battery Lane, Bethesda, MD 20814, (US)
 Van Wie, David M., 1250 Lakeside Drive, Sunnyvale, CA 94086, (US)

LEGAL REPRESENTATIVE:

Beresford, Keith Denis Lewis (28273), BERESFORD & Co. 16 High Holborn,
 London WC1V 6BX, (GB)

PATENT (CC, No, Kind, Date): EP 1555591 A2 050720 (Basic)

APPLICATION (CC, No, Date): EP 2005075672 960213;

PRIORITY (CC, No, Date): US 388107 950213

DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FR; GB; GR; IE; IT; LI; LU; MC;
 NL; PT; SE

RELATED PARENT NUMBER(S) - PN (AN):

EP 861461 (EP 96922371)

INTERNATIONAL PATENT CLASS: G06F-001/00; **G06F-017/60**

ABSTRACT WORD COUNT: 147

NOTE:

Figure number on first page: NONE

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200529	1002
SPEC A	(English)	200529	194028
Total word count - document A			195030
Total word count - document B			0
Total word count - documents A + B			195030

...INTERNATIONAL PATENT CLASS: **G06F-017/60**

...SPECIFICATION cleared or an error number if an error occurs.

Example of an SPE "Set Notification **Address** "Driver Call:

```
SPE(underscore)set(underscore)notify (long service(underscore)id, int
(fcn*receiver) (void...
```

12/3,K/2 (Item 2 from file: 348)
 DIALOG(R)File 348:EUROPEAN PATENTS
 (c) 2005 European Patent Office. All rts. reserv.

01752676

Systems and methods for secure transaction management and electronic rights protection**Systeme und Verfahren zur gesicherten Transaktionsverwaltung und elektronischem Rechtsschutz****Systemes et procedes de gestion de transactions securisees et de protection de droits electroniques**

PATENT ASSIGNEE:

ELECTRONIC PUBLISHING RESOURCES, INC., (976840), 460 Oakmead Parkway,
Sunnyvale, CA 94086-4708, (US), (Applicant designated States: all)

INVENTOR:

Ginter, Karl L., 10404 43rd Avenue, Beltsville Maryland 20705, (US)
Shear, Victor H., 5203 Battery Lane, Bethesda Maryland 20814, (US)
Spahn, Francis J., 2410 Edwards Avenue, El Cerrito California 94530, (US)
van Wie, David M., 1250 Lakeside Drive, Sunnyvale California 94086, (US)

LEGAL REPRESENTATIVE:

Smith, Norman Ian et al (36041), fJ CLEVELAND 40-43 Chancery Lane,
London WC2A 1JQ, (GB)

PATENT (CC, No, Kind, Date): EP 1431864 A2 040623 (Basic)
EP 1431864 A3 050216

APPLICATION (CC, No, Date): EP 2004075701 960213;

PRIORITY (CC, No, Date): US 388107 950213

DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FR; GB; GR; IE; IT; LI; LU; MC;
NL; PT; SE

RELATED PARENT NUMBER(S) - PN (AN):

EP 861461 (EP 96922371)

INTERNATIONAL PATENT CLASS: G06F-001/00; **G06F-017/60**

ABSTRACT WORD COUNT: 151

NOTE:

Figure number on first page: 77

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200426	1450
SPEC A	(English)	200426	166929
Total word count - document A			168379
Total word count - document B			0
Total word count - documents A + B			168379

...INTERNATIONAL PATENT CLASS: **G06F-017/60**

...SPECIFICATION cleared or an error number if an error occurs.

Example of an SPE "Set Notification **Address** "Driver Call:

SPE(underscore)set(underscore)notify (long service(underscore)id, int
(fcn*receiver) (void))

This function sets a notification **address** (receiver) for a specified
service. If the notification **address** is set to NULL, SPE device driver
736 will send notifications for packets to the...

12/3,K/3 (Item 1 from file: 349)

DIALOG(R)File 349:PCT FULLTEXT

(c) 2005 WIPO/Univentio. All rts. reserv.

01068878 **Image available**

**SYSTEMS AND METHODS FOR IDENTIFYING FRAUD AND ABUSE IN PRESCRIPTION CLAIMS
SYSTEMES ET PROCEDES DE DETECTION DES FRAUDES ET ABUS DANS L'UTILISATION
D'ORDONNANCES MEDICALES**

Patent Applicant/Assignee:

NDCHEALTH CORPORATION, One National Data Plaza, Atlanta, GA 30329-2010,
US, US (Residence), US (Nationality)

Inventor(s):

EIDEX Brian, 107 Hickory Trail, Stockbridge, GA 30281, US,
ROWE James Couser III, 352 Spring Willow Drive, Sugar Hill, GA 30518, US,

Legal Representative:

SILVERIO William R (et al) (agent), Sutherland Asbill & Brennan LLP, 999
Peachtree Street, Atlanta, GA 30309-3996, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200398400 A2-A3 20031127 (WO 0398400)
Application: WO 2003US15982 20030516 (PCT/WO US03015982)
Priority Application: US 2002381395 20020516

Designated States:

(Protection type is "patent" unless otherwise stated - for applications
prior to 2004)

AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
LS LT LU LV MA MD MG MK MN MW MX MZ NI NO NZ OM PH PL PT RO RU SC SD SE
SG SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE
SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 7272

Main International Patent Class: G06F-017/60

Fulltext Availability:

Claims

Claim

method that monitors prescription transactions for **possible** fraud and
abuse and generates messages when there is a **likelihood** that a
fraudulent transaction has occurred. Furthen-nore, it would be beneficial
if such a system allowed payers to identify reasons why a transaction is
identified as **fraudulent** so that the payers can
communicate with pharmacies to **determine** the problems identified in a
1 5 prescription transaction.

SUMMARY OF TBE INVENTION

Systems and...

...More specifically, systems and methods of the present invention
intercept and analyze prescription claims to **determine** the **likelihood**
that a claim is **fraudulent** . To effect this, the present invention
utilizes a fraud scoring engine and a ftaud management...

...The fraud scoring engine utilizes a compilation of expert rules and
profiling engine methodologies to **determine** the **likelihood** that a
prescription claim is the result of **fraudulent** or abusive behavior. The
ftaud scoring engine assigns a fraud **score** to rate the **probability**
that a claim is fraudulent in nature. The ftaud management interface is
an interface that...

...manage the claims during the recovery process.

3

Using the fraud scoring engine-generated fraud **score** , a payer, such as
an insurance company, can adjudicate a claim as normal, ask the...

...before the claim is approved for payment. Additionally, the present
invention provides a payer's **fraud** staff tools to quickly **determine**
why a claim received a particular **fraud score** so that they can
provide explanation to the pharniacist. By identifying fraud and abuse,
the...

...and the pharmacy submitting the prescription claim, analyzing the prescription claim to generate a **fraud score**, the **fraud score** based upon the 1 5 **likelihood** that the prescription claim is fraudulent, comparing the **fraud score** to business rules generated at least in part by a payer, wherein the business rules define a threshold value, and, rejecting the prescription claim as fraudulent where the **fraud score** exceeds the threshold value. According to one aspect of the invention, the method further includes the step of processing the prescription claim where the **fraud score** fails to exceed the threshold value. According to another aspect of the invention, the step...

...step of analyzing comprises the step of analyzing the prescription claim to generate a **fraud score**, wherein the **fraud score** is based at least in part upon profile information.

Furthermore, the step of analyzing can include the step of analyzing the prescription claim to generate a **fraud score**, wherein the **fraud score** is based at least in part upon short-term transaction patterns. The method can also include the step of forwarding the prescription claim to the payer where the **fraud score** fails to exceed the threshold value.

4

According to another embodiment of the present invention...

...processor functionally coupled to the means for receiving a prescription claim and configured for executing **computer**-executable instructions for: analyzing the prescription claim to generate a **fraud score**, the **fraud score** based upon the **likelihood** that the prescription claim is fraudulent; comparing the **fraud score** to business rules generated at least in part by a payer, wherein the business rules...

...0 define a threshold value; and rejecting the prescription claim as fraudulent where the **fraud score** exceeds the threshold value. According to one aspect of the present invention, the processor further includes **computer**-executable instructions for processing the prescription claim where the **fraud score** fails to exceed the threshold value. According to another 1 5 aspect of the present...

...prescription claim. According to yet another aspect of the present invention, the processor further includes **computer**-executable instructions for analyzing the prescription claim to generate a **fraud score**, wherein the **fraud score** is based at least in part upon profile information.

The processor may also include **computer**-executable instructions for analyzing the prescription claim to generate a **fraud score**, wherein the **fraud score** is based at least in part upon short-term transaction patterns. Additionally, the processor may...

...include computer-executable instructions for forwarding the prescription claim to the payer where the **fraud score** fails to exceed the threshold value.

According to yet another embodiment of the present invention...

...pharmacy POS device, wherein the means for analyzing are operable to generate a **fraud score** corresponding to the

5

prescription claim, means for comparing the **fraud score** to at least one threshold value generated at least in part by a payer, and means for rejecting the prescription claim as fraudulent where the **fraud score** exceeds the threshold value. These and other features, aspect and

embodiments of the invention will...
...processes described with
6
respect to FIG. 2 are used to screen prescription transactions for
possible fraudulent claims.
Exemplary embodiments of the present invention will hereinafter be
described with reference to...

...accordance with the present invention, the host server 104 may be
configured for performing certain **fraud** screening processes for the
detection of **possible** **fraud** and abuse (hereafter referred to
collectively as "fraudX") in a prescription transaction. More
particularly, the host server 104 examines the characteristics of a
prescription claim to **determine** the possibility that the claim is 1 0
fraudulent. In the case where the host server 104 functions as a
clearinghouse, the screening processes for **detection** of possible **fraud**
may be implemented as preprocessing and/or post-processing methods. In
other embodiments, the host...

...as "reject messages") that are transmitted to the pharmacy POS device
102 when a potential **fraudulent** transaction is **detected**. Reject
messages may indicate that a prescription claim has been rejected,
provide a pharmacist with...

...136, a database management system ("DBMS") 138
and a fraud and abuse module 140. The **fraud** and abuse module 140 may
comprise **computer**-executable instructions for performing various
screening 5 processes for **detecting** possible **fraud** in pharmacy
transactions and for managing related messaging and reporting functions.
The host server 104...

...122 evaluates a prescription claim (hereafter referred to as a "claim")
and assigns a fraud **score** and reason codes based upon the claim. The
fraud **score** is based on a compilation of fraudulent screening processes
implemented by statistical model evaluations and...

...behavior. The reason codes are assigned to a claim to describe the basis
for fraud **score**. In this regard, the reason codes are similar to reason
codes assigned to credit report scores for explaining the reason for a
particular **score**. After reception of a prescription claim transaction
(block 140), the claim transaction is parsed to...

...which a submitted daily dosage value can be derived. After the claim is
parsed to **determine** its components, the claim undergoes processing by
the **fraud** and abuse module 122, and more specifically, the claim is
compared to statistical models (blocks...
...to evaluate the pharmacy-submitted claim. Statistical models are used to
evaluate each claim to **determine** the **likelihood** that the claim is
fraudulent, and include objective statistics relating to pharmacists,
doctors and consumer. For instance, statistics could include: the
relative distance between each of the prescriber, pharmacy and consumer;
the average number of prescriptions
1...

...106 to collect the necessary comparison data to execute the evaluations.
For instance, where the **address** of a physician is **compared** to the
address of a pharmacy, a mapping or like 1 5 program may be accessed to
determine the **relative** distance between the physician
office
e and the pharmacy. Once pertinent statistical models are identified...

12/3,K/4 (Item 2 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2005 WIPO/Univentio. All rts. reserv.

00933152 **Image available**

**EXTENDED WEB ENABLED MULTI-FEATURED BUSINESS TO BUSINESS COMPUTER SYSTEM
FOR RENTAL VEHICLE SERVICES
SYSTEME INFORMATIQUE ETENDU ENTRE ENTREPRISES, A FONCTIONS MULTIPLES,
FONCTIONNANT SUR LE WEB, POUR DES SERVICES DE LOCATION DE VEHICULES**

Patent Applicant/Assignee:

THE CRAWFORD GROUP INC, 600 Corporate Park Drive, St. Louis, MO 63105, US
, US (Residence), US (Nationality), (For all designated states except:
US)

Patent Applicant/Inventor:

WEINSTOCK Timothy Robert, 1845 Highcrest Drive, St. Charles, MO 63303, US
, US (Residence), US (Nationality), (Designated only for: US)
DE VALLANCE Kimberly Amm, 2037 Silent Spring Drive, Maryland Heights, MO
63043, US, US (Residence), US (Nationality), (Designated only for: US)
HASELHORST Randall Allan, 1016 Scenic Oats Court, Imperial, MO 63052, US,
US (Residence), US (Nationality), (Designated only for: US)
KENNEDY Craig Stephen, 9129 Meadowglen Lane, St. Louis, MO 63126, US, US
(Residence), US (Nationality), (Designated only for: US)
SMITH David Gary, 10 Venice Place Court, Wildwood, MO 63040, US, US
(Residence), US (Nationality), (Designated only for: US)
TINGLE William T, 17368 Hilltop Ridge Drive, Eureka, MO 63025, US, US
(Residence), US (Nationality), (Designated only for: US)
KLOPFENSTEIN Anita K, 433 Schwarz Road, O'Fallon, IL 62269, US, US
(Residence), US (Nationality), (Designated only for: US)

Legal Representative:

HAFERKAMP Richard E (et al) (agent), HOWELL & HAFERKAMP, L.C., Suite
1400, 7733 Forsyth Blvd., St. Louis, MO 63105-1817, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200267175 A2 20020829 (WO 0267175)
Application: WO 2001US51437 20011019 (PCT/WO US0151437)
Priority Application: US 2000694050 20001020

Parent Application/Grant:

Related by Continuation to: US 2000694050 20001020 (CIP)

Designated States:

(Protection type is "patent" unless otherwise stated - for applications
prior to 2004)

AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PH PL PT RO RU SD SE SG SI SK
SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 243912

Main International Patent Class: **G06F-017/60**

Fulltext Availability:

Detailed Description

Detailed Description

... delays all of which increase the
cost of doing business and contribute to-an increased **risk** of

services being rendered in an unsatisfactory manner in many instances to the end user...R.-)

-AMRNTD (-R--)

-AMRPRD (-RU-)

-AMSURD (CR-D)

-AM0095POO (CRU-)

-AM009601 (CRU-)

-AM009701 (CR--)

@Embedded Data /Constants.

'YES,

INO I

:)cess

Brarchical numeric ID: 1. 1. 4

led name.

ne: AUT...

12/3,K/5 (Item 3 from file: 349)

DIALOG(R)File 349:PCT FULLTEXT

(c) 2005 WIPO/Univentio. All rts. reserv.

00872926 **Image available**

METHOD AND SYSTEM FOR DETECTING FRAUD

PROCEDE ET SYSTEME DE DETECTION DE FRAUDES

Patent Applicant/Assignee:

EBAY INC, 2125 Hamilton Avenue, San Jose, CA 95125, US, US (Residence),

US (Nationality), (For all designated states except: US)

Patent Applicant/Inventor:

MAY Jason, 1882 Crestmont Drive, San Jose, CA 95124, US, US (Residence),

US (Nationality), (Designated only for: US)

FLINT Ian, 1765 Drew Avenue, Mountain View, CA 94043, US, US (Residence),

US (Nationality), (Designated only for: US)

Legal Representative:

MALLIE Michael J (et al) (agent), Blakely, Sokoloff, Taylor & Zafman LLP,

7th Floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200207058 A1 20020124 (WO 0207058)

Application: WO 2001US40917 20010611 (PCT/WO US0140917)

Priority Application: US 2000615638 20000713

Designated States:

(Protection type is "patent" unless otherwise stated - for applications prior to 2004)

AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ

EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR

LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL

TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG

(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW

(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 8855

Main International Patent Class: G06F-017/60

Fulltext Availability:

Detailed Description

Detailed Description

... that the payment transaction has been rejected.

If the financial institution approves the transaction, the **fraud detection** software performs rule-based analysis, assigning a **score** for the transaction based on rule 19

violation, as shown in block 420. The list of **possible** rules is endless. Generally, certain information gleaned from the transaction information is **compared** with other information. This other information may be generally available **address** look-up information to determine whether the seller's address and the shipping and mailing...

12/3,K/6 (Item 4 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2005 WIPO/Univentio. All rts. reserv.

00851775 **Image available**

ADVANCED ASSET MANAGEMENT SYSTEMS
SYSTEMES DE GESTION D'AVOIRS PERFECTIONNES

Patent Applicant/Assignee:

VIRTUAL ASSETS INCORPORATED, 10387 Eclipse Way, Columbia, MD 21044, US,
US (Residence), US (Nationality), (For all designated states except:
US)

Patent Applicant/Inventor:

ZAMBRZYCKI John V, 1123 King Street, Redwood City, CA 94061, US, US
(Residence), US (Nationality), (Designated only for: US)
JACKSON Christopher K, 10387 Eclipse Way, Columbia, MD 21044, US, US
(Residence), US (Nationality), (Designated only for: US)
CHOIE Carolyn H, 1123 King Street, Redwood City, CA 94061, US, US
(Residence), NZ (Nationality), (Designated only for: US)
LAYMAN Kevin W, 1123 King Street, Redwood City, CA 94061, US, US
(Residence), US (Nationality), (Designated only for: US)
NEWMAN Edward J Jr, 1919 Prairie Square, Apt. 116, Schaumburg, IL 60173,
US, US (Residence), US (Nationality), (Designated only for: US)
RICHARDSON David E Jr, 1123 King Street, Redwood City, CA 94061, US, US
(Residence), US (Nationality), (Designated only for: US)

Legal Representative:

PRIDDY Robert (et al) (agent), Hall, Priddy, Myers & Vande Sande, 10220
River Road, Suite 200, Potomac, MD 20854, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200184906 A2-A3 20011115 (WO 0184906)
Application: WO 2001US15283 20010511 (PCT/WO US0115283)
Priority Application: US 2000569023 20000511

Designated States:

(Protection type is "patent" unless otherwise stated - for applications
prior to 2004)

AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS
LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ
TM TR TT TZ UA UG US UZ VN YU ZA ZW

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG

(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW

(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 124618

Main International Patent Class: **G06F-017/60**

Fulltext Availability:

Detailed Description

Detailed Description.

... and resolve wager transactions between two or more parties.

In most wagers or games of **chance** or skill, an outcome is predicted by one party. Depending on the wager or game, odds may be given. for a variety of **possible** outcomes by the same or a different party. Once the rules of the wager or...

...as to their belief or desire for or against one, some, or all of the **possible** outcomes. Wagers can be placed at the start of an event or during the course...

12/3,K/7 (Item 5 from file: 349)

DIALOG(R)File 349:PCT FULLTEXT

(c) 2005 WIPO/Univentio. All rts. reserv.

00839969

SYSTEM AND METHOD FOR DETECTING FRAUDULENT TRANSACTIONS**SYSTEME ET PROCEDE SERVANT A DETECTER DES TRANSACTIONS FRAUDULEUSES**

Patent Applicant/Assignee:

ALTICOR INC, 7575 Fulton Street East, Ada, MI 49355-0001, US, US
(Residence), US (Nationality)

Inventor(s):

HILLMER James M, 2053 Eastcastle, S.E., Grand Rapids, MI 49508, US,
JONES Richard A, 2961 Alger S.E., Grand Rapids, MI 49546, US,
GESSNER Colleen M, 3141 Boyes N.E., Grand Rapids, MI 49525, US,
JOHNSTON Connie S, 4253 Curwood, S.E., Grand Rapids, MI 49508, US,
MARTIN Norene K, 406 N. Monroe Street, Lowell, MI 49331, US,

Legal Representative:

KATZ James L (agent), Brinks Hofer Gilson & Lione, P.O. Box 10087,
Chicago, IL 60610, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200173652 A1 20011004 (WO 0173652)
Application: WO 2001US8815 20010319 (PCT/WO US0108815)
Priority Application: US 2000535298 20000324

Designated States:

(Protection type is "patent" unless otherwise stated - for applications prior to 2004)

AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE
ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT
LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM
TR TT TZ UA UG UZ VN YU ZA ZW

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG

(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW

(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 10566

Main International Patent Class: **G06F-017/60**

Fulltext Availability:

Detailed Description

Detailed Description

... be nonfraudulent. Such customer identity information may include the customer name, credit card number, **checking** account number, **address** or combinations thereof

This database 212 accounts for customers 102 who have a known good relationship with a vendor 106 but often have their transactions 100 flagged as **fraudulent** by **fraud detection** system 108 for other reasons such as a high transaction amount, shipping to a high **risk** zip code or an unusually high frequency of orders ("velocity"). As the nature of such positive information is **likely** highly confidential, such positive databases 212 and comparisons (Block 2 1 0) are preferably completed...

...customer has not committed fraud at one vendor does not necessarily mean they are not **likely** to commit fraud at another vendor. If the current customer 102 is found in the...

...transaction 100 is bypassed from further processing, and the transaction accepted (Block 230). Otherwise the **fraud detection** system continues its analysis (Block 214). In alternative embodiments, the positive identification is used to decrease the **likelihood** of a false positive result from the **fraud detection** system.

In order to further analyze the parameters I 1 6, the form of payment... transactions I 00 are not mistakenly indicated as fraudulent. The transaction I 00 is further **checked** against other **consumer information** databases 332 (Block 330). These other **consumer information** databases 332 are typically fee based and include proprietary databases of the consumer information provider...

...the amount of access charges they are comfortable incurring versus the added benefit to the **determination** of **fraud**.

If it is **determined** that the check of the alternate databases 332 has made it unlikely that the current...

...as described above (Block 338). Otherwise an indicator indicating that the current transaction 100 is **likely** fraudulent is returned to the vendor 106 (Block 338). In one embodiment, the customer **address**, card holder **address** and ship-to **address** are all **verified** against databases 332. If all three match, the fraud **score** is overridden and the transaction is approved. Alternatively, a less stringent match is required or other **verified** in place of or in addition to the **addresses**. In yet another parameters are **verified** alternative embodiment, the **authentication** results from the databases 332 are, themselves, assigned point values. Utilizing these point values, the fraud **score** is recomputed and re-compared against the fraud **score** threshold. Alternatively, the authentication results can be used to weight the point values of one or more of the transaction parameters 1 16 in the fraud multiplier computation and the **fraud score** is recomputed.

As the **fraud detection** system 108 operates, there may be errors (i.e. false positive and false negative responses...

12/3,K/8 (Item 6 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2005 WIPO/Univentio. All rts. reserv.

00806382

METHOD FOR AFFORDING A MARKET SPACE INTERFACE BETWEEN A PLURALITY OF

JMB

Date: 27-Oct-05

**MANUFACTURERS AND SERVICE PROVIDERS AND INSTALLATION MANAGEMENT VIA A
MARKET SPACE INTERFACE**
**PROCEDE DE MISE A DISPOSITION D'UNE INTERFACE D'ESPACE DE MARCHÉ ENTRE UNE
PLURALITE DE FABRICANTS ET DES FOURNISSEURS DE SERVICES ET GESTION
D'UNE INSTALLATION VIA UNE INTERFACE D'ESPACE DE MARCHÉ**

Patent Applicant/Assignee:

ACCENTURE LLP, 1661 Page Mill Road, Palo Alto, CA 94304, US, US
(Residence), US (Nationality)

Inventor(s):

MIKURAK Michael G, 108 Englewood Blvd., Hamilton, NJ 08610, US,

Legal Representative:

HICKMAN Paul L (et al) (agent), Oppenheimer Wolff & Donnelly LLP, 1400
Page Mill Road, Palo Alto, CA 94304, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200139028 A2 20010531 (WO 0139028)

Application: WO 2000US32308 20001122 (PCT/WO US0032308)

Priority Application: US 99444773 19991122; US 99444798 19991122

Designated States:

(Protection type is "patent" unless otherwise stated - for applications
prior to 2004)

AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE
ES FI GB GE GH GM HR HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV
MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT
TZ UA UG UZ VN YU ZW

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG

(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW

(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 170977

Main International Patent Class: **G06F-017/60**

Fulltext Availability:

Detailed Description

Detailed Description

... object request broker. The object request broker allows the
hiformation Services Manager to share management **information** stored in
distributed databases. The Proactive Threshold Manager uses the
information provided by the Information...

12/3,K/9 (Item 7 from file: 349)

DIALOG(R)File 349:PCT FULLTEXT

(c) 2005 WIPO/Univentio. All rts. reserv.

00801780 **Image available**

METHOD AND SYSTEM FOR DETECTING FRAUD IN NON-PERSONAL TRANSACTIONS

**PROCEDE ET SYSTEME DE DETECTION DES FRAUDES DANS DES TRANSACTIONS NON
PERSONNELLES**

Patent Applicant/Assignee:

FRAUD-CHECK COM INC, 70 West Red Oak Lane, White Plains, NY 10604, US, US
(Residence), US (Nationality)

Inventor(s):

CANDELLA George J, 348A Heritage Hills, Somers, NY 10589, US,

NOHAVEC Irene H, 48 De Motte Avenue, Clifton, NJ 07011, US,

SCRUGGS Michael L, 2020 Longtail Trail, Argyle, TX 76226-4500, US,

Legal Representative:

DE ROSA Kenneth R (agent), Wolf, Block, Schorr and Solis-Cohen LLP, 22nd

floor, 1650 Arch Street, Philadelphia, PA 19103-2097, US,
Patent and Priority Information (Country, Number, Date):

Patent: WO 200135301 A1 20010517 (WO 0135301)

Application: WO 2000US30981 20001109 (PCT/WO US0030981)

Priority Application: US 99164444 19991109

Designated States:

(Protection type is "patent" unless otherwise stated - for applications prior to 2004)

AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE
ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT
LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM
TR TT TZ UA UG UZ VN YU ZA ZW

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG

(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW

(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 6925

Main International Patent Class: G06F-017/60

Fulltext Availability:

Detailed Description

Claims

English Abstract

A method and system is disclosed for **detecting fraud** (100) in non-personal transactions. The method and system comprise transmitting the purchaser's data, includes a ship-to address for the transaction, to a **fraud - detection** system (100); processing the purchaser's data to **determine** whether the transaction is **potentially fraudulent** (102, 104, 106); and returning the **relative risks** of fraudulent activity associated with the transaction. The method and system may include any of the following additional steps: **checking** to determine whether the purchaser's ship-to **address** (122) exists, **checking** the purchaser's ship-to **address** against a historical database to **determine** whether a prior history of **fraud** (172) exists, **checking** the purchaser's ship-to **address** against an historical database to **determine** whether a pattern of **fraudulent** activity (126) exists for the ship-to **address**; and **checking** the purchaser's ship-to address against a modeling engine (128) to **determine** whether elements exist in the demographic data which correlate with **fraudulent** trends. In addition, a **score** (130) may be **calculated** based at least in part upon the **likelihood** that the transaction is fraudulent.

Detailed Description

... the purchaser's data to determine whether the transaction is potentially fraudulent; and returning the **relative risks** of fraudulent activity associated with the transaction. The method and system may include any of the following additional steps: **checking** to determine whether the purchaser's ship-to **address** exists, **checking** the purchaser's ship-to **address** against an historical database to **determine** whether a prior history of **fraud** exists, **checking** the purchaser's ship-to **address** against an historical database to **determine** whether a pattern of **fraudulent** activity exists for the ship-to **address**; and **checking** the purchaser's ship-to **address** against a modeling engine to **determine** whether elements exist in the demographic data which correlate with **fraudulent** trends.

In addition, a **score** may be **calculated** based at least in part upon

the **likelihood** that the transaction is fraudulent.

The processing step, in certain forms of the invention, comprises...

Claim

... the step of checking the purchaser's ship-to address against a modeling engine to **determine** whether elements exist in the demographic data which correlate with **fraudulent** trends.

17 The **fraud detection** method according to claim 1, further comprising the step of calculating a **score** based at least in part upon the **likelihood** that the transaction is fraudulent.

18 The fraud detection method according to claim 2, further...the step of checking the purchaser's ship-to address against a modeling engine to **determine** whether elements exist in the demographic data which correlate with **fraudulent** trends.

32 The **fraud detection** method according to claim 3 1, further comprising the step of calculating a **score** based at least in part upon the **likelihood** that the transaction is fraudulent.

12/3,K/10 (Item 8 from file: 349)

DIALOG(R)File 349:PCT FULLTEXT

(c) 2005 WIPO/Univentio. All rts. reserv.

00737987 **Image available**

GLOBALLY TIME-SYNCHRONIZED SYSTEMS, DEVICES AND METHODS

SYSTEMES GLOBALEMENT SYNCHRONISES DANS LE TEMPS

Patent Applicant/Assignee:

REVEO INC, 85 Executive Boulevard, Elmsford, NY 10523, US, US (Residence)
, US (Nationality), (For all designated states except: US)

Patent Applicant/Inventor:

FARIS Sadeg M, 24 Pocantico River Road, Pleasantville, NY 10570, US, US
(Residence), US (Nationality), (Designated only for: US)

HAMLIN Gregory J, 33 Church Street, Presque Isle, ME 04769, US, US
(Residence), US (Nationality), (Designated only for: US)

FLANNERY James P, 30 Williams Street, New City, NY 10965, US, US
(Residence), US (Nationality), (Designated only for: US)

Legal Representative:

PERKOWSKI Thomas J (agent), Soundview Plaza, 1266 East Main Street,
Stamford, CT 06902, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200050974 A2-A3 20000831 (WO 0050974)

Application: WO 2000US5093 20000228 (PCT/WO US0005093)

Priority Application: US 99258573 19990226; US 2000513601 20000225

Parent Application/Grant:

Related by Continuation to: US Not furnished (CIP)

Designated States:

(Protection type is "patent" unless otherwise stated - for applications prior to 2004)

AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB
GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA
MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA
UG US UZ VN YU ZA ZW

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE

(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG

(AP) GH GM KE LS MW SD SL SZ TZ UG ZW

(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English
Filing Language: English
Fulltext Word Count: 80968

Main International Patent Class: **G06F-017/60**

Fulltext Availability:

Claims

Claim

... 4G, the game server uses the content of the security verification log to attempt to **detect fraudulent** activities. The response notification hash is used to make sure the response sent is consistent...security considerations dictate that additional encryption and other security measures be taken to minimize the **chance** of tampering with the system. An alternative way of providing a much more accurate start...number of important advantages. For example, remote contest creation and administration creates additional opportunities and **potential** business models. In particular, administration of tests and quizzes in educational settings is an ideal...system of the present invention also includes several provisions which allow as many spectators as **possible** to view the contest and its associated advertising. Although the Internet is growing at an...

12/3,K/11 (Item 9 from file: 349)

DIALOG(R)File 349:PCT FULLTEXT

(c) 2005 WIPO/Univentio. All rts. reserv.

00736218 **Image available**

**METHOD AND APPARATUS FOR CONDUCTING COMMERCE BETWEEN INDIVIDUALS
PROCEDE ET APPAREIL PERMETTANT D'EFFECTUER DES OPERATIONS COMMERCIALES
ENTRE INDIVIDUS**

Patent Applicant/Assignee:

VISA INTERNATIONAL SERVICE ASSOCIATION, 900 Metro Center Boulevard,
Foster City, CA 94404, US, US (Residence), US (Nationality), (For all
designated states except: US)

Patent Applicant/Inventor:

MATSUDA Paul J, 220 Hazel Avenue, Mill Valley, CA 94941, US, US
(Residence), US (Nationality), (Designated only for: US)
PERRY Sarah E, 220 Hazel Avenue, Mill Valley, CA 94941, US, US
(Residence), US (Nationality), (Designated only for: US)
WILK Tracy L, 417 Sylvan Avenue, San Mateo, CA 94404, US, US (Residence),
US (Nationality), (Designated only for: US)

Legal Representative:

SCOTT Jonathan O (agent), Beyer Weaver Thomas & Nguyen, LLP, P.O. Box
130, Mountain View, CA 94042-0130, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200049554 A2 20000824 (WO 0049554)
Application: WO 2000US4348 20000218 (PCT/WO US0004348)
Priority Application: US 99135103 19990219; US 99352468 19990714

Designated States:

(Protection type is "patent" unless otherwise stated - for applications
prior to 2004)

AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB
GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA
MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA
UG US UZ VN YU ZA ZW

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 9786

Main International Patent Class: **G06F-017/60**

Fulltext Availability:

Detailed Description

Detailed Description

... 1 5 Additional checks may also be performed at this step 262. For example, an **address verification check** may be performed to **verify** that the cardholder **address** provided at step 260 is accurate and matches cardholder address records maintained by the payment...

...For example, transaction server 2 1 0 and/or financial network 220 may perform a **risk** analysis for each card registration, taking into account data elements for the present registration, such...

...nature of the participant's e-mail addresses (e.g., are they anonymous e-mail **addresses** which do not **verify** the identity of the participant?); Internet dialin location; etc. **Risk** techniques known in the art may be used to assess a **risk** variable to each transaction based on an analysis of these variables. In the event that a particular registration appears to carry a high **probability** of fraud, the registration should be aborted without generating a cardholder account record or confirmation message. For example, neural network or rule based **fraud** analysis and **detection** techniques may be used to analyze the account and to predict or **detect** fraudulent or risky activity.

1 2

In some circumstances, if the account check or status check...

12/3,K/12 (Item 10 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2005 WIPO/Univentio. All rts. reserv.

00560555 **Image available**

INTERNET BUSINESS TRANSACTION PROCESSOR

PROCESSEUR DE TRANSACTIONS COMMERCIALES SUR INTERNET

Patent Applicant/Assignee:

HARDWARESTREET COM INC,

Inventor(s):

ALVIN Robert S,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200023928 A2 20000427 (WO 0023928)

Application: WO 99US24452 19991019 (PCT/WO US9924452)

Priority Application: US 98104830 19981019; US 99345383 19990630

Designated States:

(Protection type is "patent" unless otherwise stated - for applications prior to 2004)

AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH
GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN
MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW
GH GM KE LS MW SD SL SZ TZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY
DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML

MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 7778

Main International Patent Class: **G06F-017/60**
Fulltext Availability:
Claims

Claim

... invention.

Figure 2 is a state diagram of the order processing of the present invention

Figure 3 is a flow diagram showing the **fraud** processing according to the present invention.

Figure 4 is a flow diagram showing the distributor selection processing according to the present invention...

...after the

product is ordered. As the communications technology becomes more advanced, it may be **possible** to maintain a continuous connection to the distributors' network thereby obtaining real-time status of...when a student accesses the Online

Shopping System 20 of the present invention as a **potential** customer, the Online Shopping System 20 displays a catalog of mixed products appropriate for students...

...to 10% + cost since this

is a category of products that the customer would most **likely** buy even though the price may be a little bit high. On the other hand...

...Order Processing System 30 of

the present invention is comprised of four basic sub systems: **Fraud Detection** 310, Credit Card Services 320, Distributor Selection 330, and Customer Service 340. The overall functionality...

...When an order for a selected product is received,

the Order Processing System 30 first **determines** whether the order is a valid order by the **Fraud Detection** sub system 310. If the order is valid, then the order is sent to the...order.

A detailed description of each of the sub-systems is provided hereinafter.

Multi-Level **Fraud Detection**

The **Fraud Detection** sub-system 310 of the present invention is a multi-level **fraud** checking system used to **determine** if an order is a valid order. As shown in Figure 1, when an order...

...productsf sales prices of the products, etc.

This order information is initially passed through the **Fraud Detection** sub-system 310.

The **Fraud Detection** sub-system 310 initially performs a data integrity **check** on the order information for completeness such as billing **address** information, shipping address information, and method of payment. For credit card purchases, the credit card...

...fraud check service.

Based on the information received from the financial institution, a fraud level **score**, for example, is generated. The fraud level **score** is a grading system that indicates the level of **risk** the order will pose to the business by processing the order. The **score** is then compared with a predetermined threshold or a plurality of thresholds. Each threshold serves...

...trigger to invoke

other fraud rule based checks to be performed in conjunction with the **score** to determine the total status of the failed orders. This allows the failed order to be characterized by several types of failures given a total overall **score**.

If the order passes the fraud checks, it is sent for finalized order processing. If...

...The failed orders in the sorting bin are analyzed

for reasons why the fraud level **score** was so high.

Failed orders are analyzed for previous purchases by the customer, whether the customer is an account holder, etc. and sorted between high **risk** and low **risk** orders. For instance, orders from repeat customers who otherwise have a good history of previous purchases, for example, are low **risk** orders even though the fraud **score** is high and orders from customers who have no previous purchase history pose a high **risk** on defaulting on payments. Subsequently, the sorted orders are either sent to Customer Service 340...the order is completed, the order is passed onto the Order Processing system 30.

The **Fraud Detection** sub-system 310 performs a data integrity check such as whether each of the required...

...the

corrections. If the order passes the integrity check, then the order undergoes the gross **fraud** check.

The gross **fraud** check **determines** whether the customer has a history of defaulting on payments, whether the credit card number...

...checking service such as CyberSource@.

CyberSource(D processes the order information and returns a fraud **score**. The fraud **score** is then compared to a plurality of predetermined threshold that may be modified by customer...

...As for the orders in the sort bin, the failed orders are sorted between high **risk** and low **risk** orders such as whether the order was from an account holder who has good credit history from past purchases, whether the fraud **score** was too high because the billing address did not match the address of the credit modifications and variations are **possible** in light of the above teaching. The preferred embodiment was chosen and described in order...

Set	Items	Description
S1	83733	FRAUD? OR DECEPTION? OR THEFT OR THIEV? OR LARCENY OR STEA- L? OR ROBBERY OR CHEAT? OR SWINDL? OR DISHONEST?
S2	5808633	DETECT??? OR CALCULAT? OR DETERMIN? OR COMPUT??? OR FIGURE- ??? OR ESTIMAT? OR GAUG?
S3	2452124	POTENTIAL? OR LIKELIHOOD OR RELATIVE OR POSSIBL? OR PROBAB- LE OR PROBABILITY OR LIKELY
S4	2015672	CHECK??? OR COMPAR??? OR VERIFY? OR VERIFI? OR CONFIRM??? - OR VALIDAT? OR AFFIRM? OR CORROBORAT? OR AUTHENTICAT?
S5	386944	(PURCHASER? OR BUYER? OR SHOPPER? OR CONSUMER? OR CUSTOMER? OR USER?)(1W)(DATA OR INFO OR INFORMATION) OR SHIP()TO OR SH- IPPING OR BILL()TO OR ADDRESS? OR AREA()CODE? OR PHONE()NUMBE- R? OR ZIP
S6	272638	RISK OR RISKS OR CHANCE OR SCORE
S7	8899	S1(S)S2
S8	1280	S7(S)S3
S9	39795	S4(S)S5
S10	21	S8 AND S9
S11	2	S10 AND S6
S12	11	S10 NOT PY>1999
S13	10	RD (unique items)
File	2:INSPEC	1898-2005/Oct W3 (c) 2005 Institution of Electrical Engineers
File	35:Dissertation Abs Online	1861-2005/Oct (c) 2005 ProQuest Info&Learning
File	65:Inside Conferences	1993-2005/Oct W4 (c) 2005 BLDSC all rts. reserv.
File	99:Wilson Appl. Sci & Tech Abs	1983-2005/Sep (c) 2005 The HW Wilson Co.
File	474:New York Times Abs	1969-2005/Oct 26 (c) 2005 The New York Times
File	475:Wall Street Journal Abs	1973-2005/Oct 26 (c) 2005 The New York Times
File	583:Gale Group Globalbase(TM)	1986-2002/Dec 13 (c) 2002 The Gale Group

13/5/1 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC
(c) 2005 Institution of Electrical Engineers. All rts. reserv.

07116991 INSPEC Abstract Number: C9902-7120-003

Title: Using a genetic algorithm based classifier system for modeling auditor decision behavior in a fraud setting

Author(s): Welch, O.J.; Reeves, T.E.; Welch, S.T.

Author Affiliation: Sch. of Bus. & Adm., St Mary's Univ., San Antonio, TX, USA

Journal: International Journal of Intelligent Systems in Accounting, Finance and Management vol.7, no.3 p.173-86

Publisher: Wiley,

Publication Date: Sept. 1998 Country of Publication: UK

CODEN: IJAMEN ISSN: 1055-615X

SICI: 1055-615X(199809)7:3L.173:UGAB;1-U

Material Identity Number: P932-98004

Language: English Document Type: Journal Paper (JP)

Treatment: Practical (P)

Abstract: This paper **addresses** a classification problem involving the decisions of Defense Contractor Audit Agency (DCAA) auditors when they are **estimating the likelihood of fraud** by contractors developing bids for government contracts. The objective of the study is to investigate if this decision involves non-algebraic processes associated with a posited simultaneous decision model or algebraic processes posited by sequential decision processes. We propose that in classification decision models involving simultaneous processing, genetic algorithms represent an innovative heuristic approach, which may produce improved models when **compared** to traditional mathematical approaches. (20 Refs)

Subfile: C

Descriptors: decision support systems; financial data processing; fraud; genetic algorithms

Identifiers: genetic algorithm based classifier system; auditor decision behavior; fraud setting; Defense Contractor Audit Agency auditors; contractors; government contracts; nonalgebraic processes; posited simultaneous decision model; algebraic processes; sequential decision processes; classification decision models; innovative heuristic approach

Class Codes: C7120 (Financial computing); C1180 (Optimisation techniques); C7102 (Decision support systems)

Copyright 1998, IEE

13/5/2 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC
(c) 2005 Institution of Electrical Engineers. All rts. reserv.

06912348 INSPEC Abstract Number: C9806-5210B-060

Title: CASPER: Concurrent hardware-software co-synthesis of hard real-time aperiodic and periodic specifications of embedded system architectures

Author(s): Dave, B.P.; Jha, N.K.

Author Affiliation: Dept. of Electr. Eng., Princeton Univ., NJ, USA

Conference Title: Proceedings. Design, Automation and Test in Europe (Cat. No.98EX123) p.118-24

Publisher: IEEE Comput. Soc, Los Alamitos, CA, USA

Publication Date: 1998 Country of Publication: USA xxxiv+993 pp.

ISBN: 0 8186 8359 7 Material Identity Number: XX98-00366

U.S. Copyright Clearance Center Code: 0 8186 8359 7/98/\$10.00

Conference Title: Proceedings Design, Automation and Test in Europe

Conference Sponsor: Eur. Design & Autom. Assoc. - EDAA; Electron. Design Autom. Consortium - EDAC; IEEE Comput. Soc. Tech. Comm. Test Technol.; IFIP

- Working Group on CAD - IFIP 10.5; Eur. CAD Standards Initiative - ECSI; ACM-SIGDA; AEIA; ATI; CEPIS; CLCR; CNR; IEEE CS DATC; GI; GMM; HTE; ITG; KVIV; MATE; NIISAPRAN

Conference Date: 23-26 Feb. 1998 Conference Location: Paris, France

Language: English Document Type: Conference Paper (PA)

Treatment: Theoretical (T)

Abstract: Hardware-software co-synthesis of an embedded system requires mapping of its specifications into hardware and software modules such that its real-time and other constraints are met. Embedded system specifications are generally represented by acyclic task graphs. Many embedded system applications are characterized by aperiodic as well as periodic task graphs. Aperiodic task graphs can arrive for execution at any time and their resource requirements vary depending on how their constituent tasks and edges are allocated. Traditional approaches based on a fixed architecture coupled with slack **stealing** and/or on-line **determination** of how to serve aperiodic task graphs are not suitable for embedded systems with hard real-time constraints, since they cannot guarantee that such constraints would always be met. In this paper, we **address** the problem of concurrent co-synthesis of aperiodic and periodic specifications of embedded systems. We **estimate** the resource requirements of aperiodic task graphs and allocate execution slots on processing elements and communication links for executing them. Our approach guarantees that the deadlines of both aperiodic and periodic task graphs are always met. We have observed that simultaneous consideration of aperiodic task graphs while performing co-synthesis of periodic task graphs is vital for achieving superior results **compared** to the traditional slack **stealing** and dynamic scheduling approaches. To the best of our knowledge, this is the first co-synthesis algorithm which provides simultaneous support of periodic and aperiodic task graphs with hard real-time constraints. Application of the proposed algorithm to several examples from real-life telecom transport systems shows that up to 28% and 34% system cost savings are **possible** over co-synthesis algorithms which employ slack **stealing** and rate-monotonic scheduling, respectively. (18 Refs)

Subfile: C

Descriptors: computer architecture; directed graphs; high level synthesis; real-time systems

Identifiers: CASPER; concurrent hardware-software co-synthesis; real-time specification; embedded system architecture; acyclic task graph; aperiodic task graph; periodic task graph; telecom transport system

Class Codes: C5210B (Computer-aided logic design); C5220 (Computer architecture); C1160 (Combinatorial mathematics)

Copyright 1998, IEE

13/5/3 (Item 3 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2005 Institution of Electrical Engineers. All rts. reserv.

06605695 INSPEC Abstract Number: C9707-7120-028

Title: **Smarter, more secure smartcards**

Author(s): Blythe, I.

Journal: BYTE (International Edition) vol.22, no.6 p.63-4

Publisher: McGraw-Hill,

Publication Date: June 1997 Country of Publication: USA

CODEN: BYTEDJ ISSN: 0360-5280

SICI: 0360-5280(199706)22:6L:63:SMSS;1-F

Material Identity Number: G109-97004

Language: English Document Type: Journal Paper (JP)

Treatment: Practical (P); Product Review (R)

Abstract: Take an early personal **computer** from the '80s, some memory and squeeze it all into a single chip that's only 25 square millimeters

(about 0.04 square inches) in size. This is a smartcard IC, which itself is embedded in a plastic blank the size of a credit card. This card then acts as an intelligent memory device that stores and transfers its contents securely, even under **potential** attacks. Applications currently using smartcards include telephone cards, health cards, pay TV, banking, loyalty schemes, GSM (Global System for Mobile communications) and other cellular telephones, network log-in/ **authentication**, and data security. The increasing added value within these applications brings new threats of **fraud** and loss. SGS-Thomson's ST19 is a new family of smartcard ICs that **addresses** this need for higher security. The ST19 series builds on the experience and security aspects of the ST16 smartcard IC family. (0 Refs)

Subfile: C

Descriptors: security of data; smart cards

Identifiers: personal computer; smartcard IC; intelligent memory device; data security; SGS-Thomson's ST19

Class Codes: C7120 (Financial computing); C6130S (Data security)

Copyright 1997, IEE

13/5/4 (Item 4 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2005 Institution of Electrical Engineers. All rts. reserv.

06426096 INSPEC Abstract Number: C9701-7210L-002

Title: The use of electronic book theft detection systems in libraries

Author(s): Witt, T.B.

Journal: Journal of Interlibrary Loan, Document Delivery & Information Supply vol.6, no.4 p.45-60

Publisher: Haworth Press,

Publication Date: 1996 Country of Publication: USA

CODEN: JLDSED ISSN: 1072-303X

SICI: 1072-303X(1996)6:4L:45:EBTD;1-5

Material Identity Number: B090-96004

Language: English Document Type: Journal Paper (JP)

Treatment: Practical (P)

Abstract: The current popular trend in library security is the installation of electronic book **theft detection** systems to combat the attempted removal of library materials that have not been **checked** -out at the circulation desk. Although these systems have been reported to deter **theft** by library patrons, no electronic book **theft detection** system is foolproof. To rely solely on an electronic system to provide collection security is foolish. To truly ensure the security of a library collection, a total security program is necessary. This program must also **address** the issue of **potential theft** of materials by employees. (98 Refs)

Subfile: C

Descriptors: library automation; personnel; security

Identifiers: electronic book theft detection systems; library security; library materials; circulation desk; library patrons; collection security; security program; employees

Class Codes: C7210L (Library automation)

Copyright 1996, IEE

13/5/5 (Item 5 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2005 Institution of Electrical Engineers. All rts. reserv.

06154315 INSPEC Abstract Number: B9602-6200-009, C9602-7410F-080

Title: Knowledge discovery in telecommunication services data using Bayesian network models

Author(s): Ezawa, K.J.; Norton, S.W.
Author Affiliation: AT&T Bell Labs., Murray Hill, NJ, USA
Conference Title: KDD-95 Proceedings. First International Conference on Knowledge Discovery and Data Mining p.100-5
Editor(s): Fayyad, U.M.; Uthurusamy, R.
Publisher: AAAI, Menlo Park, CA, USA
Publication Date: 1995 Country of Publication: USA xiv+345 pp.
ISBN: 0 929280 82 2 Material Identity Number: XX95-01994
Conference Title: Proceedings of First International Conference on Knowledge Discovery and Data Mining (KDD-95)
Conference Sponsor: AAAI; AT&T Global Inf. Solutions; GTE Lab.; et al
Conference Date: 20-21 Aug. 1995 Conference Location: Montreal, Que., Canada

Language: English Document Type: Conference Paper (PA)

Treatment: Practical (P)

Abstract: **Fraud** and uncollectible debt are multi billion dollar problems in the telecommunications industry. Because it is difficult to know which accounts will go bad, we are faced with the difficult knowledge discovery task of characterizing a rare binary outcome using large amounts of noisy, high dimensional data. Binary characterizations may be of interest but will not be especially useful in this domain. Instead, proposing an action requires an **estimate** of the **probability** that a customer or a call is uncollectible. The paper **addresses** the discovery of predictive knowledge bearing on **fraud** and uncollectible debt using a supervised machine learning method that constructs Bayesian network models. The new method is able to predict rare event outcomes and cope with the quirks and copious amounts of input data. The Bayesian network models it produces serve as an input module to a normative decision support system and suggest ways to reinforce or redirect existing efforts in the problem area. We **compare** the performance of several conditionally independent models with the conditionally dependent models discovered by the new learning system using real world datasets of 4-6 million records and 600-800 million bytes. (20 Refs)

Subfile: B C

Descriptors: Bayes methods; decision support systems; knowledge acquisition; learning (artificial intelligence); telecommunication computing; telecommunication services

Identifiers: knowledge discovery; telecommunication services data; Bayesian network models; uncollectible debt; fraud; telecommunications industry; rare binary outcome; binary characterizations; predictive knowledge bearing; supervised machine learning method; rare event outcomes; conditionally independent models; real world datasets

Class Codes: B6200 (Telecommunication); C7410F (Communications computing); C1140Z (Other topics in statistics); C6170K (Knowledge engineering techniques); C7102 (Decision support systems); C1240 (Adaptive system theory)

Copyright 1996, IEE

13/5/6 (Item 6 from file: 2)
DIALOG(R)File 2:INSPEC
(c) 2005 Institution of Electrical Engineers. All rts. reserv.

05968864 INSPEC Abstract Number: B9507-6210L-099, C9507-5620-026

Title: Avoiding an impersonation attack on a communications network

Author(s): Russell, S.

Author Affiliation: Fac. of Inf. Technol., Queensland Univ. of Technol., Brisbane, Qld., Australia

Journal: EDPACS vol.23, no.1 p.1-17

Publication Date: July 1995 Country of Publication: USA

CODEN: EDPCDF ISSN: 0736-6981

Language: English Document Type: Journal Paper (JP)

Treatment: Practical (P)

Abstract: Communications network problems arise in connection with, or are associated with the use of public key encryption and the realization of electronic data interchange, electronic funds transfer, and electronic currency. Little attention has been given to the **potential** damage from an impersonation attack upon a communications network by an insider working in collusion with a wiretapper. When connection with other organizations is allowed, maintaining complete control over the extended system, including the communications network and the remote **computing** facility, is not **possible**. The threat in such an environment that some incoming documents will be **frauds** created by an impersonator should be removed. The article **addresses** that need and offers help in meeting it. It begins by defining and illustrating wiretap impersonation attacks, goes on to consider conventional **authentication** methods and their underlying theories, **addresses** the problem of reliable **verification** in an attack in which a wiretapper colludes with one of more members of the organisation, presents current solution to that problem as well as some of the various objections to them, and concludes with a model designed to **detect** any attempted **deception** through such collusion. (0 Refs)

Subfile: B C

Descriptors: computer crime; computer networks; fraud; message authentication

Identifiers: impersonation attack; communications network problems; public key encryption; electronic data interchange; electronic funds transfer; electronic currency; wiretapper; remote computing facility; wiretap impersonation attacks; authentication methods; reliable verification

Class Codes: B6210L (Computer communications); C5620 (Computer networks and techniques); C6130S (Data security); C0310D (Computer installation management)

Copyright 1995, IEE

13/5/7 (Item 7 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2005 Institution of Electrical Engineers. All rts. reserv.

04764642 INSPEC Abstract Number: B90077730, C90070339

Title: Multiparty computation with faulty majority

Author(s): Beaver, D.; Goldwasser, S.

Author Affiliation: Harvard Univ., Cambridge, MA, USA

Conference Title: Advances in Cryptology - CRYPTO '89. Proceedings p. 589-90

Editor(s): Brassard, G.

Publisher: Springer-Verlag, Berlin, West Germany

Publication Date: 1990 Country of Publication: West Germany xiii+634 pp.

ISBN: 3 540 97317 6

Conference Sponsor: Int. Assoc. Cryptologic Res.

Conference Date: 20-24 Aug. 1989 Conference Location: Santa Barbara, CA, USA

Language: English Document Type: Conference Paper (PA)

Treatment: Theoretical (T)

Abstract: The authors **address** the problem of performing a multiparty computation when more than half of the processors are cooperating Byzantine faults. They show how to **compute** any boolean function of n inputs distributively, preserving the privacy of inputs held by nonfaulty processors, and ensuring that faulty processors obtain the function value 'if and only if' the nonfaulty processors do. If the nonfaulty processors

do not obtain the correct function value, they **detect cheating** with high **probability**. The solution is based on a new type of **verifiable** secret sharing in which the secret is revealed not all at once but in small increments. This slow-revealing process ensures that all processors discover the secret at roughly the same time. The solution assumes the existence of an oblivious transfer protocol and uses broadcast channels. They do not require that the processors have equal **computing** power. (10 Refs)

Subfile: B C

Descriptors: cryptography; fault tolerant computing; multiprocessing systems; protocols

Identifiers: faulty majority; multiparty computation; Byzantine faults; boolean function; privacy; verifiable secret sharing; slow-revealing process; oblivious transfer protocol; broadcast channels

Class Codes: B6120B (Codes); B6150 (Communication switching theory); C5620 (Computer networks and techniques); C5470 (Performance evaluation and testing); C6130 (Data handling techniques)

13/5/8 (Item 1 from file: 35)

DIALOG(R)File 35:Dissertation Abs Online

(c) 2005 ProQuest Info&Learning. All rts. reserv.

01488156 ORDER NO: AADAA-I9619488

MECHANISMS OF UNDERREPORTING OF DIETARY INTAKE (OBESITY, FOOD RECORDS)

Author: MUHLHEIM, LAUREN SIEGLER

Degree: PSY.D.

Year: 1995

Corporate Source/Institution: RUTGERS THE STATE UNIVERSITY OF NEW JERSEY, G.S.A.P.P. (0542)

Chairperson: G. TERENCE WILSON

Source: VOLUME 57/02-B OF DISSERTATION ABSTRACTS INTERNATIONAL.
PAGE 1449. 118 PAGES

Descriptors: PSYCHOLOGY, CLINICAL ; PSYCHOLOGY, BEHAVIORAL

Descriptor Codes: 0622; 0384

Previous research has documented widespread underreporting of dietary intake, especially among obese persons. The purpose of the present study was to investigate **possible** psychological explanations for this phenomenon. Fifty subjects reporting inability to lose weight despite low self-reported caloric intake were recruited by the Obesity Research Center for an energy balance and metabolism study designed to help **determine** the source of their difficulty losing weight. Two investigations **addressing** this issue were conducted. The first investigation utilized a bogus pipeline paradigm to **determine** whether the accuracy of self-reported intake would improve when subjects were given an incentive to be more accurate. Twenty-eight subjects completed one-week food diaries under standard conditions. Then, 17 subjects were entered into the experimental condition and asked to keep two week food diaries while being told the researcher was **verifying** their intake through the use of doubly labeled water. Eleven subjects in the control group were asked merely to self-monitor for two more weeks. Analysis of the data suggests that subjects in the experimental group reported significantly greater dietary intake than control subjects, when controlling for self-reported intake during the screening phase. Thus, the bogus pipeline was found to improve the accuracy of patients' self-reported intake. However, even under the bogus pipeline, subjects continued to significantly underreport their dietary intake. The second investigation tested hypotheses about the psychological mechanisms responsible for misreporting. Forty-two subjects completed one-week food diaries as well as a battery of psychological

questionnaires measuring self- **deception** , impression management, and fear of negative evaluation. Analysis of the data indicates that only the Marlowe-Crowne Social Desirability Scale was significantly correlated with underreporting of caloric intake, although the majority of measures did correlate positively with underreporting. Results suggest that underreporting of dietary intake is a complex process in which impression management plays a role. At least a portion of the underreporting of caloric intake by overweight persons seems to be a conscious attempt to manage their presentation to others in a world that is increasingly critical of overweight persons. Limitations to and implications of the findings are discussed.

13/5/9 (Item 1 from file: 474)

DIALOG(R)File 474:New York Times Abs

(c) 2005 The New York Times. All rts. reserv.

00231646 NYT Sequence Number: 085389711208

(Berlinger repts that he has submitted 59 cases of apparent welfare fraud in NYC to city welfare officials; discloses plans to investigate absent fathers, saying he believes that 'thousands' of cases involved only alleged abandonment so family could go on relief; notes he also plans to investigate welfare clients who hold jobs that they do not disclose, aliens who may have returned to their own countries but continue to receive welfare checks at local address , recipients who receive aid from different welfare centers under different names and clients and landlords who fail to return security deposits for welfare apartments; indicates he is checking possible 'malfeasance or misfeasance' on part of middle-level welfare admrs in duplicate- check frauds estimated to have cost city \$4.5-million in '70)

New York Times, Col. 6, Pg. 110

Wednesday December 8 1971

DOCUMENT TYPE: Newspaper JOURNAL CODE: NYT LANGUAGE: English

RECORD TYPE: Abstract

DESCRIPTORS: BANKS AND BANKING; CHECK FRAUDS; FRAUDS AND SWINDLING; HOUSING; IMMIGRATION AND EMIGRATION; LABOR; RENTING AND LEASING; WELFARE (US); WELFARE RECIPIENTS, EMPLOYMENT OF
PERSONAL NAMES: BERLINGER, GEORGE F; KIHSS, PETER
GEOGRAPHIC NAMES: NEW YORK CITY; NEW YORK STATE; UNITED STATES (1971)

13/5/10 (Item 1 from file: 583)

DIALOG(R)File 583:Gale Group Globalbase(TM)

(c) 2002 The Gale Group. All rts. reserv.

03414003

SECURITY IS A PRIME CONCERN AT FRANCE TELECOM

FRANCE - SECURITY IS A PRIME CONCERN AT FRANCE TELECOM

Messages Des PTT (MDP) 0 March 1990 p37-38

ISSN: 0245-6001

Language: French

France Telecom (France) has the largest **computer** installation in France and is constantly aware of the possibility of **fraudulent** misuse of its systems as well as human error and **possible** damage to equipment. In 1989, damage to **computer** installations in France amounted to at least FF10 bil, and five years ago France Telecom set up STT, a telecommunications security service which co- ordinates all France Telecom's security activities. Vital functions such as payroll, accounts, telephone billing

and the networks themselves are all managed by **computer**. The CNET (Centre national d'etudes de France Telecom) has developed SAS (serveur d'accès sécurisé) which automatically **checks** the **address** of a terminal to ensure that all access to a **computer** is authorised. The user then has to enter a password. Another security measure requires the user to identify himself and then enter a password or memory card to prove his authenticity. If an incorrect password is entered three times, the card becomes invalid. This same principle is used for France Telecom's Pastel cards which allows the cost of calls made in telephone boxes to be charged to the caller's personal telephone account. France Telecom also encourages staff to make regular back-ups of **computer** data and ensure that **computer** viruses do not affect an entire system.

PRODUCT: Computer & Data Security Software (7372CD); CAD/CAM Mechanical Software (COSW);

EVENT: COMPANIES ACTIVITIES (10);

COUNTRY: France (4FRA); Northern Europe (414); OECD Europe (415); European Economic Community Countries (419); NATO Countries (420); South East Asia Treaty Organisation (913);

Set	Items	Description
S1	83733	FRAUD? OR DECEPTION? OR THEFT OR THIEV? OR LARCENY OR STEA- L? OR ROBBERY OR CHEAT? OR SWINDL? OR DISHONEST?
S2	5808633	DETECT??? OR CALCULAT? OR DETERMIN? OR COMPUT??? OR FIGURE- ??? OR ESTIMAT? OR GAUG?
S3	2452124	POTENTIAL? OR LIKELIHOOD OR RELATIVE OR POSSIBL? OR PROBAB- LE OR PROBABILITY OR LIKELY
S4	2015672	CHECK??? OR COMPAR??? OR VERIFY? OR VERIFI? OR CONFIRM??? - OR VALIDAT? OR AFFIRM? OR CORROBORAT? OR AUTHENTICAT?
S5	386944	(PURCHASER? OR BUYER? OR SHOPPER? OR CONSUMER? OR CUSTOMER? OR USER?) (1W) (DATA OR INFO OR INFORMATION) OR SHIP()TO OR SH- IPPING OR BILL()TO OR ADDRESS? OR AREA()CODE? OR PHONE()NUMBE- R? OR ZIP
S6	272638	RISK OR RISKS OR CHANCE OR SCORE
S7	8899	S1(S)S2
S8	1280	S7(S)S3
S9	39795	S4(S)S5
S10	21	S8 AND S9
S11	2	S10 AND S6
S12	11	S10 NOT PY>1999
S13	10	RD (unique items)
S14	1482620	NON()PERSONAL OR NONPERSONAL OR ELECTRONIC OR ON()LINE OR - ONLINE OR INTERNET OR DIGITAL?
S15	1448120	TRANSACTION? OR SALE? OR COMMERCE OR SHOP? OR RETAIL? OR - SELLING OR PURCHAS? OR MARKETING
S16	52039	S14(3N)S15
S17	193	S16 AND S7
S18	5	S17 AND S9
S19	5114	S14 AND S1
S20	62	S19 AND S9
S21	18	S20 NOT PY>1999
S22	18	RD (unique items)
File	2:INSPEC 1898-2005/Oct W3	(c) 2005 Institution of Electrical Engineers
File	35:Dissertation Abs Online 1861-2005/Oct	(c) 2005 ProQuest Info&Learning
File	65:Inside Conferences 1993-2005/Oct W4	(c) 2005 BLDSC all rts. reserv.
File	99:Wilson Appl. Sci & Tech Abs 1983-2005/Sep	(c) 2005 The HW Wilson Co.
File	474:New York Times Abs 1969-2005/Oct 26	(c) 2005 The New York Times
File	475:Wall Street Journal Abs 1973-2005/Oct 26	(c) 2005 The New York Times
File	583:Gale Group Globalbase(TM) 1986-2002/Dec 13	(c) 2002 The Gale Group

22/5/1 (Item 1 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2005 Institution of Electrical Engineers. All rts. reserv.

07390781 INSPEC Abstract Number: B1999-12-6120D-012, C1999-12-6130S-017

Title: Secure fingerprinting using public-key cryptography

Author(s): Yoshiura, H.; Sasaki, R.; Takaragi, E.

Author Affiliation: Syst. Dev. Lab., Hitachi Ltd., Yokohama, Japan

Conference Title: Security Protocols. 6th International Workshop.
Proceedings p.83-9

Editor(s): Christianson, B.; Crispo, B.; Harbison, W.S.; Roe, M.

Publisher: Springer-Verlag, Berlin, Germany

Publication Date: 1999 Country of Publication: Germany viii+239 pp.

ISBN: 3 540 65663 4 Material Identity Number: XX-1999-01936

Conference Title: Security Protocols. 6th International Workshop

Conference Date: 15-17 April 1998 Conference Location: Cambridge, UK

Language: English Document Type: Conference Paper (PA)

Treatment: Practical (P)

Abstract: Fingerprinting is a process that embeds identifiers of the **buyers** of **data** into the data. It enables buyers who copied and redistributed data illegally to be identified from the redistributed data. An essential requirement for fingerprinting is the prevention of false accusations, i.e., honest buyers should not be accused even when **fraud** has been committed by merchants and third parties. Previous fingerprinting methods either could not meet this requirement or met it at a high cost, such as that associated with the use of independent servers for fingerprinting. The paper proposes to embed buyers' **digital** signatures into data and to identify illegal buyers by **verifying** signatures in the redistributed data. The security of the signature **verification** is discussed, assuming that the redistributed data have been modified by the illegal buyers. The paper shows that the proposed method can prevent false accusations at an acceptable cost. (10 Refs)

Subfile: B C

Descriptors: fingerprint identification; **fraud** ; protocols; public key cryptography

Identifiers: secure fingerprinting; public key cryptography; data buyers; redistributed data; false accusations; honest buyers; **fraud** ; third parties; merchants; fingerprinting methods; independent servers; **digital** signatures; illegal buyers; signature verification; acceptable cost

Class Codes: B6120D (Cryptography); B6150M (Protocols); C6130S (Data security); C1260C (Cryptography theory); C5640 (Protocols)

Copyright 1999, IEE

22/5/2 (Item 2 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2005 Institution of Electrical Engineers. All rts. reserv.

07328709

Title: Flood warnings

Author(s): Austin, D.

Journal: Banking Technology vol.16, no.6 p.28-31

Publisher: IBC Business Publishing,

Publication Date: July-Aug. 1999 Country of Publication: UK

CODEN: BATEEM ISSN: 0266-0865

SICI: 0266-0865(199907/08)16:6L:28:FW;1-#

Material Identity Number: K580-1999-006

Language: English Document Type: Journal Paper (JP)

Treatment: Practical (P); Product Review (R)

Abstract: With card not present **fraud** figures on the rise, serious

questions are being asked about the safety of the **Internet** as a channel for commerce, and about the commitment of banks to reducing losses. (0 Refs)

Subfile: D

Descriptors: commerce; **fraud** ; **Internet**

Identifiers: card not present **fraud** ; **Internet** **Fraud** Watch; e-commerce; banks; loss reduction; small business; repeat billings; secure sockets layer encryption; restaurant; scam; con artists; cramming; **online** shopping; stolen credit card; smart card; **digital** certificate; downloadable software; **fraudulent** orders; cardholder **address** **verification** ; AVS system; **fraud** countermeasures

Class Codes: D2050 (Financial applications); D5020 (Computer networks and intercomputer communications)

Copyright 1999, IEE

22/5/3 (Item 3 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2005 Institution of Electrical Engineers. All rts. reserv.

07261500

Title: Comfort level [electronic commerce security]

Author(s): Haigh, T.; Ross, B.

Journal: Electronic Commerce World vol.9, no.3 p.30-2

Publisher: EDI World,

Publication Date: March 1999 Country of Publication: USA

CODEN: ECWOFD ISSN: 1092-0366

SICI: 1092-0366(199903)9:3L:30:CLEC;1-O

Material Identity Number: G344-1999-004

Language: English Document Type: Journal Paper (JP)

Treatment: Practical (P)

Abstract: There are almost as many methods and models of securing **electronic** transactions as there are e-commerce sites on the **Internet** . The problem with creating a standard or a single solution for protecting e-commerce is that there are different and sometimes conflicting goals in securing an e-commerce transaction. The goals of the merchant may not be the same as the goals of the user or bank. The merchant wants to have a valid transaction, cover liability, and receive payment for goods and services. The users would like to purchase products, protect their private information (name, **address** , payment information, etc.), and pay for only the products they have agreed to purchase. The institutions providing payment would like to detect and avoid **fraud** , protect the users from merchants, and protect the merchants from users. There are many solutions in use that cover one or more of these security goals, and where one solution provides privacy, another may provide only transaction **validation**

(0 Refs)

Subfile: D

Descriptors: data privacy; **electronic** commerce; security of data

Identifiers: **electronic** transaction security; e-commerce; valid transaction; cover liability; payment; private information protection; **fraud** ; privacy; **electronic** commerce

Class Codes: D2140 (Marketing, retailing and distribution); D2050E (Banking); D1060 (Security); D1040 (Human aspects)

Copyright 1999, IEE

22/5/4 (Item 4 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2005 Institution of Electrical Engineers. All rts. reserv.

06912348 INSPEC Abstract Number: C9806-5210B-060

Title: CASPER: Concurrent hardware-software co-synthesis of hard real-time aperiodic and periodic specifications of embedded system architectures

Author(s): Dave, B.P.; Jha, N.K.

Author Affiliation: Dept. of Electr. Eng., Princeton Univ., NJ, USA

Conference Title: Proceedings. Design, Automation and Test in Europe (Cat. No.98EX123) p.118-24

Publisher: IEEE Comput. Soc, Los Alamitos, CA, USA

Publication Date: 1998 Country of Publication: USA xxxiv+993 pp.

ISBN: 0 8186 8359 7 Material Identity Number: XX98-00366

U.S. Copyright Clearance Center Code: 0 8186 8359 7/98/\$10.00

Conference Title: Proceedings Design, Automation and Test in Europe

Conference Sponsor: Eur. Design & Autom. Assoc. - EDAA; Electron. Design Autom. Consortium - EDAC; IEEE Comput. Soc. Tech. Comm. Test Technol.; IFIP - Working Group on CAD - IFIP 10.5; Eur. CAD Standards Initiative - ECSI; ACM-SIGDA; AEIA; ATI; CEPIS; CLCR; CNR; IEEE CS DATC; GI; GMM; HTE; ITG; KVIV; MATE; NIISAPRAN

Conference Date: 23-26 Feb. 1998 Conference Location: Paris, France

Language: English Document Type: Conference Paper (PA)

Treatment: Theoretical (T)

Abstract: Hardware-software co-synthesis of an embedded system requires mapping of its specifications into hardware and software modules such that its real-time and other constraints are met. Embedded system specifications are generally represented by acyclic task graphs. Many embedded system applications are characterized by aperiodic as well as periodic task graphs. Aperiodic task graphs can arrive for execution at any time and their resource requirements vary depending on how their constituent tasks and edges are allocated. Traditional approaches based on a fixed architecture coupled with slack **stealing** and/or **on-line** determination of how to serve aperiodic task graphs are not suitable for embedded systems with hard real-time constraints, since they cannot guarantee that such constraints would always be met. In this paper, we **address** the problem of concurrent co-synthesis of aperiodic and periodic specifications of embedded systems. We estimate the resource requirements of aperiodic task graphs and allocate execution slots on processing elements and communication links for executing them. Our approach guarantees that the deadlines of both aperiodic and periodic task graphs are always met. We have observed that simultaneous consideration of aperiodic task graphs while performing co-synthesis of periodic task graphs is vital for achieving superior results **compared** to the traditional slack **stealing** and dynamic scheduling approaches. To the best of our knowledge, this is the first co-synthesis algorithm which provides simultaneous support of periodic and aperiodic task graphs with hard real-time constraints. Application of the proposed algorithm to several examples from real-life telecom transport systems shows that up to 28% and 34% system cost savings are possible over co-synthesis algorithms which employ slack **stealing** and rate-monotonic scheduling, respectively. (18 Refs)

Subfile: C

Descriptors: computer architecture; directed graphs; high level synthesis ; real-time systems

Identifiers: CASPER; concurrent hardware-software co-synthesis; real-time specification; embedded system architecture; acyclic task graph; aperiodic task graph; periodic task graph; telecom transport system

Class Codes: C5210B (Computer-aided logic design); C5220 (Computer architecture); C1160 (Combinatorial mathematics)

Copyright 1998, IEE

22/5/5 (Item 5 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2005 Institution of Electrical Engineers. All rts. reserv.

06806533

Title: Target: point of sale

Author(s): Marlin, S.

Journal: Bank Systems + Technology vol.35, no.1 p.36-8, 40, 42

Publisher: Miller Freeman,

Publication Date: Jan. 1998 Country of Publication: USA

CODEN: BSYTEE ISSN: 1045-9472

SICI: 1045-9472(199801)35:1L.36:TPS;1-O

Material Identity Number: N682-97017

Language: English Document Type: Journal Paper (JP)

Treatment: Economic aspects (E)

Abstract: The payments industry is seeking solutions that will balance consumer preferences for **check** writing against demands by retailers for relief from **check - fraud** losses and high paper processing costs. While banks and other institutions are enhancing paper- **check** processing systems with such technologies as **electronic check** presentment and imaging, other solutions are being advanced that would replace paper **checks** with automated clearing house or other **electronic** transactions. There is widespread agreement that getting paper out of the system is the key to **addressing** merchant needs. The challenge, though, is getting consumers to change their time-honored payment habits. (0 Refs)

Subfile: D

Descriptors: cheque processing; EFTS; **fraud** ; point of sale systems

Identifiers: payments industry; check writing; retailers; check **fraud** losses; paper processing costs; banks; **electronic** check presentment; **electronic** check imaging; automated clearing house transactions; **electronic** transactions; merchant needs

Class Codes: D2140 (Marketing, retailing and distribution); D1060 (Security); D2050E (Banking)

Copyright 1998, IEE

22/5/6 (Item 6 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2005 Institution of Electrical Engineers. All rts. reserv.

06426096 INSPEC Abstract Number: C9701-7210L-002

Title: The use of electronic book theft detection systems in libraries

Author(s): Witt, T.B.

Journal: Journal of Interlibrary Loan, Document Delivery & Information Supply vol.6, no.4 p.45-60

Publisher: Haworth Press,

Publication Date: 1996 Country of Publication: USA

CODEN: JLDSED ISSN: 1072-303X

SICI: 1072-303X(1996)6:4L.45:EBTD;1-5

Material Identity Number: B090-96004

Language: English Document Type: Journal Paper (JP)

Treatment: Practical (P)

Abstract: The current popular trend in library security is the installation of **electronic book theft** detection systems to combat the attempted removal of library materials that have not been **checked** -out at the circulation desk. Although these systems have been reported to deter **theft** by library patrons, no **electronic book theft** detection system is foolproof. To rely solely on an **electronic** system to provide collection security is foolish. To truly ensure the security of a library collection, a total security program is necessary. This program must also **address** the issue of potential **theft** of materials by employees. (98 Refs)

Subfile: C

Descriptors: library automation; personnel; security
Identifiers: **electronic** book **theft** detection systems; library security; library materials; circulation desk; library patrons; collection security; security program; employees
Class Codes: C7210L (Library automation)
Copyright 1996, IEE

22/5/7 (Item 7 from file: 2)
DIALOG(R)File 2:INSPEC
(c) 2005 Institution of Electrical Engineers. All rts. reserv.

06405835 INSPEC Abstract Number: B9612-6250F-095
Title: GSM digital cellular telephone system a case study of encryption algorithms
Author(s): Smith, T.
Author Affiliation: Centre for Telecommun. Inf. Networking, Adelaide Univ., SA, Australia
Conference Title: Mobile Communications. Technology, Tools, Applications, Authentication and Security. IFIP World Conference on Mobile Communications p.285-98
Editor(s): Encarnacao, J.L.; Rabey, J.M.
Publisher: Chapman & Hall, London, UK
Publication Date: 1996 Country of Publication: UK ix+342 pp.
ISBN: 0 412 75580 7 Material Identity Number: XX96-02563
Conference Title: Proceedings of 1996 World Conference on Mobile Communications
Conference Date: 2-6 Sept. 1996 Conference Location: Canberra, ACT, Australia
Language: English Document Type: Conference Paper (PA)
Treatment: General, Review (G); Theoretical (T)
Abstract: There have been many reports in the newspapers of eavesdropping and cloning of telephones in the analogue network. This paper investigates **digital** networks, specifically GSM, to see if they are free from these attacks. Security was seen as a high priority and was **addressed** in the development of GSM, however **fraud** in GSM has not been eliminated, in fact due to the flexibility and the new services it introduced GSM has created new forms of **fraud**. GSM includes three algorithms for the purposes of **authentication**, air interface encryption and key delivery (A3, A5 and A8). The paper looks at the history of the algorithms and the different versions. (0 Refs)
Subfile: B
Descriptors: cellular radio; cryptography; **digital** radio; **fraud**; history; message authentication; telecommunication services
Identifiers: GSM **digital** cellular telephone system; encryption algorithms; **fraud**; authentication; air interface encryption; key delivery; history
Class Codes: B6250F (Mobile radio systems); B6120B (Codes); B6210D (Telephony)
Copyright 1996, IEE

22/5/8 (Item 8 from file: 2)
DIALOG(R)File 2:INSPEC
(c) 2005 Institution of Electrical Engineers. All rts. reserv.

05968864 INSPEC Abstract Number: B9507-6210L-099, C9507-5620-026
Title: Avoiding an impersonation attack on a communications network
Author(s): Russell, S.
Author Affiliation: Fac. of Inf. Technol., Queensland Univ. of Technol.,

Brisbane, Qld., Australia

Journal: EDPACS vol.23, no.1 p.1-17

Publication Date: July 1995 Country of Publication: USA

CODEN: EDPCDF ISSN: 0736-6981

Language: English Document Type: Journal Paper (JP)

Treatment: Practical (P)

Abstract: Communications network problems arise in connection with, or are associated with the use of public key encryption and the realization of **electronic** data interchange, **electronic** funds transfer, and **electronic** currency. Little attention has been given to the potential damage from an impersonation attack upon a communications network by an insider working in collusion with a wiretapper. When connection with other organizations is allowed, maintaining complete control over the extended system, including the communications network and the remote computing facility, is not possible. The threat in such an environment that some incoming documents will be **frauds** created by an impersonator should be removed. The article **addresses** that need and offers help in meeting it. It begins by defining and illustrating wiretap impersonation attacks, goes on to consider conventional **authentication** methods and their underlying theories, **addresses** the problem of reliable **verification** in an attack in which a wiretapper colludes with one of more members of the organisation, presents current solution to that problem as well as some of the various objections to them, and concludes with a model designed to detect any attempted **deception** through such collusion. (0 Refs)

Subfile: B C

Descriptors: computer crime; computer networks; **fraud** ; message authentication

Identifiers: impersonation attack; communications network problems; public key encryption; **electronic** data interchange; **electronic** funds transfer; **electronic** currency; wiretapper; remote computing facility; wiretap impersonation attacks; authentication methods; reliable verification

Class Codes: B6210L (Computer communications); C5620 (Computer networks and techniques); C6130S (Data security); C0310D (Computer installation management)

Copyright 1995, IEE

22/5/9 (Item 9 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2005 Institution of Electrical Engineers. All rts. reserv.

03845117 INSPEC Abstract Number: D87001063

Title: **Disguising dollars**

Journal: ABA Banking Journal vol.79, no.1 p.77-8

Publication Date: Jan. 1987 Country of Publication: USA

CODEN: ABAJD5 ISSN: 0194-5947

Language: English Document Type: Journal Paper (JP)

Treatment: General, Review (G); Practical (P)

Abstract: Data encryption and message **authentication** are coming to the fore in banking. Which approach is best? When weighing the tradeoffs between encryption and **authentication**, bank security officers often mention the audit trail left behind with **authentication**. Until recently, encryption and especially message **authentication** were subjects being **addressed** mostly by the largest money center banks. Now, large regional banks have started to take action. Many observers believe that both technologies will become widely implemented by the 1990s. Although reduction of risks is the main reason for banks to use encryption and **authentication** technologies, so far the risk is a perceived one. That is, to date no major funds transfer **frauds** have occurred that involve the

type of wiretapping or other communications breaches that encryption and **authentication** are designed to prevent. The increasing reliance on **electronic** funds transfers, though, heightens the need for **electronic** security measures. Indeed, without them, expanded use of EFT would be unlikely. (0 Refs)

Subfile: D

Descriptors: banking; computer crime; EFTS; security of data

Identifiers: data encryption; message authentication; banking; security officers; audit trail; regional banks; risks; funds transfer **frauds** ; **electronic** funds transfers; **electronic** security measures; EFT

Class Codes: D1060 (Security); D2050E (Banking)

22/5/10 (Item 10 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2005 Institution of Electrical Engineers. All rts. reserv.

03777359 INSPEC Abstract Number: C87002339

Title: Fault-tolerant control of access to shared data in cached-DASD storage systems

Journal: IBM Technical Disclosure Bulletin vol.28, no.12 p.5457-9

Publication Date: May 1986 Country of Publication: USA

CODEN: IBMTAA ISSN: 0018-8689

Language: English Document Type: Journal Paper (JP)

Treatment: Practical (P)

Abstract: When two heat processors share data, a processor which is updating a portion of it must prevent the other processor from reading or updating that portion. A cached-DASD (direct-access storage device) system includes storage directors which place data into a subsystem memory or cache having a test-and-set register (TS), so that one processor only may 'own' TS and its data at once. The paper **addresses** the problem which arises when, due to a communication failure, the limiting caching or TS accessing director becomes nonoperational in that it prevents access to cache by the other director. The solution is to allow any operational director to 'steal' TS from the accessing director. This action requires a limited caching storage director to **check** before each directory access that it still 'owns' TS since the other storage director may have 'stolen' it. (0 Refs)

Subfile: C

Descriptors: **digital** storage; fault tolerant computing; multiprocessing systems

Identifiers: fault-tolerant control; shared data; cached-DASD storage systems; heat processors; direct-access storage device; storage directors; test-and-set register; communication failure

Class Codes: C5320 (Digital storage); C5440 (Multiprocessor systems and techniques)

22/5/11 (Item 11 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2005 Institution of Electrical Engineers. All rts. reserv.

03291754 INSPEC Abstract Number: B84043913

Title: A switched/broadcast ISDN to decrease user observability

Author(s): Pfitzmann, A.

Author Affiliation: Inst. fur Informatik IV, Univ. Karlsruhe, Karlsruhe, West Germany

Conference Title: 1984 International Zurich Seminar on Digital Communications. Applications of Source Coding, Channel Coding and Secrecy Coding. Proceedings p.183-90

Publisher: IEEE, New York, NY, USA
Publication Date: 1984 Country of Publication: USA xi+201 pp.
Conference Sponsor: IEEE
Conference Date: 6-8 March 1984 Conference Location: Zurich, Switzerland

Language: English Document Type: Conference Paper (PA)

Treatment: Applications (A); Practical (P)

Abstract: A switching/broadcast network structure (SBNS) is derived, which decreases user observability. The SBNS is physically based on cheap and powerful microelectronics and the enormous bandwidth and inherent broadcast facility of local networks and, logically based on the generation of random numbers and keys of a public key cryptosystem. The backbone of the SBNS proposal is a packet switched ISDN. The terminals of the switched ISDN are gateways. Each gateway masters a local two-way broadcast network which connects the user stations of a user group. Implementations of local two-way broadcast networks are discussed and protocols derived, which together can hide the sender and receiver of a message but enable the generation of untraceable return **addresses**, **digital** signatures and billing. Costs, fault tolerance, and protection against **fraud** are discussed. It is shown how patterns in time of the message traffic can be reduced. Otherwise, patterns in time could be used to monitor user behaviour, too. The SBNS is **compared** with the only other known solution to the traffic analysis problem. The other solution is found to be too costly in terms of required bandwidth. (28 Refs)

Subfile: B

Descriptors: communication networks; cryptography; **digital** communication systems; packet switching

Identifiers: costs; switched/broadcast ISDN; user observability; switching/broadcast network structure; SBNS; microelectronics; local networks; random numbers; public key cryptosystem; packet switched ISDN; gateways; sender; receiver; message; **digital** signatures; billing; fault tolerance; protection; **fraud**; patterns; traffic analysis

Class Codes: B6210M (ISDN); B6230F (Integrated switching and transmission systems)

22/5/12 (Item 12 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2005 Institution of Electrical Engineers. All rts. reserv.

03146753 INSPEC Abstract Number: B83062281, C83042036

Title: Automatic addressing of telemetry channels

Author(s): Lucero, L.A.

Author Affiliation: Sandia Nat. Labs., Livermore, CA, USA

Conference Title: ITC/USA/'82. International Telemetering Conference p.861-72

Publisher: Int. Found. Telemetering, Woodland Hills, CA, USA

Publication Date: 1982 Country of Publication: USA 917 pp.

ISBN: 0 87664 703 4

Conference Sponsor: Int. Found. Telemetering

Conference Date: 28-30 Sept. 1982 Conference Location: San Diego, CA, USA

Language: English Document Type: Conference Paper (PA)

Treatment: Applications (A)

Abstract: Using the DMA function of the RCA 1802 microprocessor, once initialized, **addressing** of telemetry channels is automatic, requiring no software. In this report the automatic **addressing** scheme is **compared** with an earlier technique that uses software. In comparison, the automatic **addressing** scheme effectively increases the software capability of the microprocessor, simplifies telemetry dataset encoding, eases dataset

changes, and may reduce the **electronic** hardware count. **Addressing** is performed using direct memory access cycle **stealing** technique. The present version of the scheme uses a section of PROM reserved for telemetry channel **addresses**. Encoding for a dataset is accomplished by programming the PROM with channel **addresses** in the order in which they are to be monitored. (1 Refs)

Subfile: B C

Descriptors: communication channels; PROM; telemetering systems

Identifiers: DMA function; RCA 1802 microprocessor; addressing of telemetry channels; automatic addressing scheme; telemetry dataset encoding; direct memory access cycle **stealing**; PROM

Class Codes: B6210J (Telemetry); B7210F (Telemetering systems); C3370Z (Other communication techniques); C7410F (Communications)

22/5/13 (Item 1 from file: 583)

DIALOG(R)File 583:Gale Group Globalbase(TM)

(c) 2002 The Gale Group. All rts. reserv.

09133758

Credit card charges hit **online** sales

UK: **ONLINE** SALES AFFECTED BY CREDIT CARD CHARGES

Computer Weekly (CRW) 08 Jul 1999 p.8

Language: ENGLISH

According to IT market research firm Gartner Group, **online** sales are being hit by high levels of credit card chargebacks, caused when purchasers dispute charges and demand refunds from their credit card companies. Companies operating **online** e-commerce sites are often experiencing chargebacks of around 15% to 30%, **compared** to traditional retailers which experience an average of 1%. Gartner claims that **online** merchants will face huge losses unless they **address** the potential increase in costs associated with **fraud** and chargebacks.

COMPANY: GARTNER GROUP

PRODUCT: Commercial Banks (6020); Consumer Finance Institutions (6140);

Nonbank Credit Card Firms (6141);

EVENT: Labour Information (53); Company Reports & Accounts (83);

COUNTRY: United Kingdom (4UK);

22/5/14 (Item 2 from file: 583)

DIALOG(R)File 583:Gale Group Globalbase(TM)

(c) 2002 The Gale Group. All rts. reserv.

09055605

Hongkong Post accepts Certificate Authority role

HONG KONG: CA ROLE AFFIRMED BY HONGKONG POST

Computerworld HK (XDP) 21 Jan 1999 Network World,p.I

Language: ENGLISH

The Information Technology and Broadcasting Bureau's invitation to Hongkong Post to set up the first certificate authority (CA) in Hong Kong has been **affirmed** by the latter. Hongkong Post will accept the role as a public CA who will guarantee safe **Internet** delivery of personal/commercial sensitive information against prohibited access and **fraud**. Besides that, the public CA will also promote e-commerce by delivering a secured environment to **address** basic e-commerce issues like integrity, authenticity and confidentiality.

COMPANY: **INTERNET** ; HONGKONG POST

PRODUCT: Computer & Data Security Software (7372CD); Intruder Prevention Systems (3662IP);
EVENT: National Government Economics (94); Plant/Facilities/Equipment (44);
COUNTRY: Hong Kong (9HON);

22/5/15 (Item 3 from file: 583)

DIALOG(R)File 583:Gale Group Globalbase(TM)
(c) 2002 The Gale Group. All rts. reserv.

06185823

'Authenticating' mobile calls

UK: AUTHENTICATION SOFTWARE UNVEILED
The Australian (XAA) 01 Aug. 1995 P.33
Language: ENGLISH

Given the rising mobile phone **theft**, Vodafone has come up with what it calls an **authentication** software that could prevent the phone from being actively cloned. When a subscriber uses a conventional analogue phone, two signals would be sent, namely, its **phone number** and serial number. When the **authentication** software is attached to the phone, it will send three signals (its **phone number**, an **electronic** serial number and a quasi-**electronic** serial number) to the Vodafone's network for identification. Hence, if a thief clones the phone, it will not be accepted by the network because it will carry the old quasi-ESN. The company announced that all new analogue phones connected to Vodafone will be equipped with the **Authentication** software while existing subscribers may have theirs converted by putting in a special code.

PRODUCT: Cellular Radio Equipment (3662CE); Computer Services (7370);
EVENT: Product Design & Development (33);
COUNTRY: United Kingdom (4UK);

22/5/16 (Item 4 from file: 583)

DIALOG(R)File 583:Gale Group Globalbase(TM)
(c) 2002 The Gale Group. All rts. reserv.

05182341

Foiling the forgers

UK - CREDIT CARD TRANSACTION VALIDATION PROFILED
Financial Times (C) 1992 (FT) 9 July 1992 p16

Retailers and banks have adopted varying methods of **validating** credit card transactions in different parts of the world. All, however, **address** the universal problem of growing credit card **fraud**. Losses from card **fraud** have risen alarmingly over the past two years. Visa International measured **fraud** and counterfeit losses on its credit cards last year at Dollars 623.4m, up 52 per cent from 1990. In the UK, the Home Office estimates card **fraud** cost Pounds 165m last year, up from Pounds 150.3m in 1990. Technology is widely seen as the chief weapon in the fight against card **cheats**, but applications must take account of regional differences. Automated signature **verification** holds greater promise in markets where credit card signatures are routinely **checked**, whereas in the US, the process would have to be disguised to make it acceptable to cardholders, who see this type of authorisation as an insult to their integrity. AEA

Technology, a unit of the former Atomic Energy Authority, has developed a signature **verification** system based upon a 'neural network' - an array of computing elements that mimics the thought processes of the human mind. Rather than simply analysing elements of the signature, like a conventional computer system, the 'Harwell Countermatch' also views the signature as a whole in the way as a person might get an overall impression of its appearance. The signature is mapped against a sample which can be recorded on the magnetic strip or semiconductor memory in a credit card. The AEA system overcomes one of the drawback's of automatic signature **verification** by learning as it goes and picking up on the natural variations in a signature. So the accuracy of the system improves. Barclaycard, the largest issuer of credit cards in the UK, is testing signature **verification**, voice recognition and fingerprint matching. All are seen as long-term ways to avoid credit card **fraud** at the point of sale. Nobody in the credit card industry sees signature **verification** as the sole solution to credit card **fraud** and there is a broad consensus that the focus of prevention must move away from the point of sale toward authorisation networks. The UK's high telecommunications costs are therefore a serious drawback, inhibiting merchants and bankers from accessing remote data processing centers.**

Copyright: Financial Times Ltd 1992

COMPANY: AEA TECHNOLOGY

PRODUCT: Data Processing in Retail Sector (7374RT); Computer Services (COSV); **Electronic** Banking Services (6005); Computer & Data Security Software (7372CD); Computer Software (COSW); Artificial Intelligence Software (7372AI);

EVENT: MARKET & INDUSTRY NEWS (60); PRODUCT DESIGN & DEVELOPMENT (33);

COUNTRY: United Kingdom (4UK); OECD Europe (415); European Economic Community Countries (419); NATO Countries (420); South East Asia Treaty Organisation (913);

22/5/17 (Item 5 from file: 583)

DIALOG(R)File 583:Gale Group Globalbase(TM)

(c) 2002 The Gale Group. All rts. reserv.

02802087

ELECTRONIC APPLICATIONS IN RETAILING INCREASE

WORLD - **ELECTRONIC** APPLICATIONS IN RETAILING INCREASE

Computerwoche (CWE) 12 May 1989 p58-61

ISSN: 0170-5121

Language: German

This 3-page report reviews the uses of **electronic** technology in retailing, citing examples in Japan, the US and Europe. **Electronic** tagging, scanning, **check** -out systems, anti- **theft** devices, sales monitoring and ordering by cards/and/or terminals. Some retailers are using video displays to market their goods, working on the principle that many shoppers make decisions at the point of sale. There is particular interest in anti- **theft** devices as 1-1.5% of turnover is lost this way. Karstadt (W Germany) has compiled a databank of regular **customers** with **information** on their lifestyle and purchases as a guide to target markets. According to the Berlin Sparkasse, automatic cash-points have quadrupled turnover. Providing the terminals costs DM3-12 k/y.

PRODUCT: **Electronic** Point of Sale Systems (3573EP);

EVENT: MARKET & INDUSTRY NEWS (60);

COUNTRY: Earth - Planet (0W);

22/5/18 (Item 6 from file: 583)
DIALOG(R)File 583:Gale Group Globalbase(TM)
(c) 2002 The Gale Group. All rts. reserv.

01364127

ERNST & WHINNEY SYSTEM TO DETECT **FRAUDS** IN BP FLOTATION
UK - ERNST & WHINNEY SYSTEM TO DETECT **FRAUDS** IN BP FLOTATION
Computing (CNG) 8 October 1987 p1

Ernst & Whinney's system TRIAL (Tracking and reporting of illegal applications for litigation) developed with Southward Computer Services, is to be run on Prime minicomputers, Compaq micros and IBM mainframes. TRIAL is to detect multiple applications for BP shares and consists of two parts: a name and **address** sorter and a cheque **checker**.

PRODUCT: **Electronic** Financial Services Sys (3573EF);
EVENT: MARKET & INDUSTRY NEWS (60);
COUNTRY: United Kingdom (4UK); OECD Europe (415); NATO Countries (420);
South East Asia Treaty Organisation (913);

Set	Items	Description
S1	933043	FRAUD? OR DECEPTION? OR THEFT OR THIEV? OR LARCENY OR STEA- L? OR ROBBERY OR CHEAT? OR SWINDL? OR DISHONEST?
S2	7311985	DETECT??? OR CALCULAT? OR DETERMIN? OR COMPUT??? OR FIGURE- ??? OR ESTIMAT? OR GAUG?
S3	6578684	POTENTIAL? OR LIKELIHOOD OR RELATIVE OR POSSIBL? OR PROBAB- LE OR PROBABILITY OR LIKELY
S4	4861379	CHECK??? OR COMPAR??? OR VERIFY? OR VERIFI? OR CONFIRM??? - OR VALIDAT? OR AFFIRM? OR CORROBORAT? OR AUTHENTICAT?
S5	2355272	(PURCHASER? OR BUYER? OR SHOPPER? OR CONSUMER? OR CUSTOMER? OR USER?)(1W)(DATA OR INFO OR INFORMATION) OR SHIP()TO OR SH- IPPING OR BILL()TO OR ADDRESS? OR AREA()CODE? OR PHONE()NUMBE- R? OR ZIP
S6	4231457	RISK OR RISKS OR CHANCE OR SCORE
S7	30606	S1(5N)S2
S8	2384	S7(S)S3
S9	18970	S4(5N)S5
S10	55	S8 AND S9
S11	39	S10 AND S6
S12	5	S11 NOT PY>1999
S13	4	RD (unique items)

File 20:Dialog Global Reporter 1997-2005/Oct 27
(c) 2005 Dialog

13/3,K/1

DIALOG(R)File 20:Dialog Global Reporter
(c) 2005 Dialog. All rts. reserv.

06387436 (USE FORMAT 7 OR 9 FOR FULLTEXT)

UC Card of Japan Selects Nestor's PRISM to Protect Against Credit Card Fraud

BUSINESS WIRE

July 26, 1999

JOURNAL CODE: WBWE LANGUAGE: English RECORD TYPE: FULLTEXT

WORD COUNT: 711

(USE FORMAT 7 OR 9 FOR FULLTEXT)

... the company's technology and success in our market," said a Manager of Security and **Risk** Management Department at UC Card. "We firmly believe that the technology and Nestor's custom...

...an exceptional level of fraud protection. Nestor's proven success in the Japanese market further **validates** their technology and expertise in **addressing** fraud issues worldwide."

PRISM Credit is an intelligent **risk** management system that provides early and accurate credit card fraud detection by identifying suspect activity...

...transactions, as well as activity across an entire portfolio. The system then produces a fraud **score** that reflects the **likelihood** that the transaction is fraudulent. High scoring transactions are routed to a fraud reviewer who...

13/3,K/2

DIALOG(R)File 20:Dialog Global Reporter
(c) 2005 Dialog. All rts. reserv.

03628441 (USE FORMAT 7 OR 9 FOR FULLTEXT)

Carreker-Antinori Announces New Trac2Fraud and Trac2ECP Product Suites

BUSINESS WIRE

December 02, 1998

JOURNAL CODE: WBWE LANGUAGE: English RECORD TYPE: FULLTEXT

WORD COUNT: 868

(USE FORMAT 7 OR 9 FOR FULLTEXT)

... Conference in Las Vegas, Nevada. Trac2Fraud is a comprehensive suite of software solutions designed to **detect** and report **potentially fraudulent** check activity. Trac2ECP is an integrated suite of products designed to deliver ECP functionality. Both are delivered on an integrated client-server platform.

"Historically, products that **address** **check** losses, electronic **check** presentment, automated hold placement, image exchange, and automated adjustments have not been cost effective for...

... public filings with the Securities and Exchange Commission by Carreker-Antinori, including those discussed under "**Risk** Factors" in Carreker-Antinori's Prospectus dated May 20, 1998.

(a) These modules currently under...

13/3,K/3

DIALOG(R)File 20:Dialog Global Reporter

(c) 2005 Dialog. All rts. reserv.

02887311

CyberSource Announces CyberSource IVS 3.0. The Fraud Screen Providing the Most Precise Protection From Internet Credit Card Fraud

PR NEWSWIRE

September 22, 1998

JOURNAL CODE: WPRW LANGUAGE: English RECORD TYPE: FULLTEXT

WORD COUNT: 1035

Web Merchants Gain Dynamic, Granular Controls for Identifying and Combating Credit Card Fraud **Risk** LOS ANGELES, Sept. 22 /PRNewswire/ -- Zeroing in on Internet credit card fraud, CyberSource(R) Corporation...

... profitability and control fraud to less than 1%. Conventional fraud detection schemes, such as the **Address Verification Service (AVS)** which is only available for US cardholders, are largely ineffective in the anonymous...

... of the Internet. While other emerging Internet fraud screen offerings tend to provide 'cookie-cutter' **risk** assessment methods that presume a similar profile for all merchants and product categories, CyberSource IVS

... enables merchants to customize a fraud screen unique to their business and specify the **risk** threshold they are willing to accept by product, or product category. The merchant may change...

... card account status is in jeopardy of being revoked. Further, CyberSource IVS accurately assesses fraud **risk** before the order is consummated, which is far more cost-effective than dealing with fraud...

...the credit card authorization process, uses data supplied with the order and artificial intelligence to " **score** " the **potential risk** of each transaction -- typically in less than five seconds. "With digitally delivered products, you are **potentially** exposed to fraud on an alarming scale, yet CyberSource's IVS technology has allowed us...

... we are able to tweak any number of variables, such as assigning different levels of **risk** for differently priced products. CyberSource IVS 3.0 looks highly promising with its even more...

... IVS 3.0 enhancements CyberSource IVS 3.0 enables a Web merchant to dynamically set **risk** assessment parameters to match their business needs. A merchant can set these parameters uniformly across...

... purchase hours" , transactions performed during the expected purchase hours (purchaser's location) are assigned no **risk** while transactions performed outside of expected purchase hours are applied a **risk score** .

* Bill to/Ship to variance -- determines whether the geographic proximity of the ship-to and bill-to addresses should be a component of the CyberSource IVS **score** (accommodates products that are often purchased as gifts and shipped to an address other than...

13/3,K/4

DIALOG(R)File 20:Dialog Global Reporter

(c) 2005 Dialog. All rts. reserv.

02887310

CyberSource and Paymentech Join Forces to Provide Robust Payment Capability and Attack Credit Card Fraud

PR NEWSWIRE

September 22, 1998

JOURNAL CODE: WPRW LANGUAGE: English RECORD TYPE: FULLTEXT

WORD COUNT: 1156

... a marketing agreement aimed at providing a robust payment processing capability that dramatically reduces the **risk** of Internet credit card fraud. The announcement was made at the Internet Commerce Expo in...

... or electronically downloadable products and services are both vulnerable, digital goods merchants are at particular **risk** because the goods are already "out the door" before a fraudulent transaction can even start...

... weighted scores and compares those scores against a merchant's defined threshold. The higher the **score**, the higher the **risk** that the attempted transaction is fraudulent. With this approach, the merchant is able to decide the level of **risk** he wishes to accept. For example, a merchant can decide that a **score** of 25 or higher indicates an unacceptable **risk** for orders placed between midnight and 5:00 a.m., yet is acceptable during daylight hours. "Traditional **fraud detection** mechanisms used for mail and telephone orders, such as the **address verification** service (AVS), simply aren't effective in the anonymous environment of the Internet," said Steve...

...president of Payment Industry Alliances at CyberSource. "CyberSource IVS goes a lot deeper than just **verifying** addresses. Rather, it examines a multitude of variables to spot the tell-tale footprints of identity...

Set	Items	Description
S1	124234	FRAUD? OR DECEPTION? OR THEFT OR THIEV? OR LARCENY OR STEA- L? OR ROBBERY OR CHEAT? OR SWINDL? OR DISHONEST?
S2	1644650	CALCULAT? OR DETERMIN? OR COMPUT??? OR FIGURE??? OR ESTIMA- T? OR GAUG?
S3	1064933	POTENTIAL? OR LIKELIHOOD OR RELATIVE OR POSSIBL? OR PROBAB- LE OR PROBABILITY OR LIKELY
S4	939415	CHECK??? OR COMPAR??? OR VERIFY? OR VERIFI? OR CONFIRM??? - OR VALIDAT? OR AFFIRM? OR CORROBORAT? OR AUTHENTICAT?
S5	541196	(PURCHASER? OR BUYER? OR SHOPPER? OR CONSUMER? OR CUSTOMER? OR USER?) (1W) (DATA OR INFO OR INFORMATION) OR SHIP()TO OR SH- IPPING OR BILL()TO OR ADDRESS? OR AREA()CODE? OR PHONE()NUMBE- R? OR ZIP
S6	905236	RISK OR RISKS OR CHANCE OR SCORE
S7	28355	S2(4N)S3
S8	4049	S4(4N)S5
S9	907	S7 AND S1
S10	13	S9 AND S8
S11	6	S10 NOT PY>1999
S12	5	RD (unique items)

File 613:PR Newswire 1999-2005/Oct 27
(c) 2005 PR Newswire Association Inc

File 813:PR Newswire 1987-1999/Apr 30
(c) 1999 PR Newswire Association Inc

File 634:San Jose Mercury Jun 1985-2005/Oct 26
(c) 2005 San Jose Mercury News

File 624:McGraw-Hill Publications 1985-2005/Oct 27
(c) 2005 McGraw-Hill Co. Inc

12/3,K/1 (Item 1 from file: 613)
DIALOG(R)File 613:PR Newswire
(c) 2005 PR Newswire Association Inc. All rts. reserv.

00188796 19991005SFTU167 (USE FORMAT 7 FOR FULLTEXT)
Inabyte Introduces InaEmailCheck; Active-X Component Instantly Tests Status of Email Addresses
PR Newswire
Tuesday, October 5, 1999 17:26 EDT
JOURNAL CODE: PR LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 442

TEXT:

...for the Win32(R) architecture, today released an Active-X component that immediately tests and **verifies** email **addresses**. InaEmailCheck is a valuable tool for e-commerce providers and other web-based businesses that need to **confirm** the validity of email **addresses** in order to complete mass mailings or execute online transactions. InaEmailCheck can be embedded directly...

...as a standalone utility. Companies that maintain large-scale email databases can use InaEmailCheck to **verify** and cull **addresses** on their lists quickly and efficiently. InaEmailCheck can also be used to **verify** **addresses** before a mass mailing, saving time and minimizing bounce-backs.

"For e-commerce companies and...

...as telephone numbers," said Mark Hennessy, president of Inabyte. "InaEmailCheck enables the immediate assessment and **verification** of virtually any email **address**. It's an efficient tool for keeping email databases up to date. Plus, by having the ability to **determine** the status of a **potential** customer's email address, online companies can cut down on input errors, improve communications and reduce the likelihood of **fraud**."

12/3,K/2 (Item 1 from file: 813)
DIALOG(R)File 813:PR Newswire
(c) 1999 PR Newswire Association Inc. All rts. reserv.

1048746 DATU009
Finjan Software and Check Point Software Technologies Tighten Java Security

DATE: January 28, 1997 15:15 EST WORD COUNT: 1,059

... automatically downloaded hostile Java applets that carry out malicious attacks, including industrial espionage, e-mail **fraud**, resource **theft**, or unnoticed alteration of information, among many other problematic and counterproductive activities. SurfinGate closely examines...

... applications into the FireWall-1 enterprise security solution to manage functions such as access control, **address** translation, **authentication**, auditing, accounting, encryption and content security. With OPSEC, all

facets of enterprise security are defined...

... the new world of Internet/intranet downloadables, and Finjan solutions protect enterprise and stand-alone **computer** resources from the **potential** risks of downloadables such as Java applets. With a dynamic group of technology specialists and...

12/3,K/3 (Item 2 from file: 813)
DIALOG(R)File 813:PR Newswire
(c) 1999 PR Newswire Association Inc. All rts. reserv.

0483869 SJ001A
**WORLD'S FIRST COMMERCIAL APPLICATION OF NEURAL NETWORK CHIP READS CHECKS
LIKE THE HUMAN EYE**

DATE: June 3, 1992 11:01 EDT WORD COUNT: 1,333

...document recognition and processing problems, from handwriting and thumbprint recognition to evaluating money for counterfeit **fraud**.

Key Benefits of Onyx

-- High Reliability: Onyx's wide tolerance for check slide speed eliminates...

...even more efficiently in the future. During its development process, the chip was exposed, through **computer** simulation, to all **possible** combinations and permutations of MICR characters. As a result, the chip learned to distinguish good...

...real-world problem -- namely, the need to improve both the speed and accuracy of the **check** acceptance process. Onyx **addresses** this need by employing advanced neural network technology.

Functionality and Availability

Onyx is part of....

12/3,K/4 (Item 1 from file: 634)
DIALOG(R)File 634:San Jose Mercury
(c) 2005 San Jose Mercury News. All rts. reserv.

08358270
**FAKE FIRMS STEAL COMPUTER GOODS OLD SCAM: AFTER PRODUCTS ARE RECEIVED,
SWINDLERS DISAPPEAR WITHOUT PAYING; PROFITABLE CRIME IS LESS RISKY THAN
HOLDUPS, COPS NOTE.**

San Jose Mercury News (SJ) - Sunday, December 24, 1995
By: RAOUL V. MOWATT, Mercury News Staff Writer
Edition: Morning Final Section: Local Page: 1B
Word Count: 1,038

**FAKE FIRMS STEAL COMPUTER GOODS OLD SCAM: AFTER PRODUCTS ARE RECEIVED,
SWINDLERS DISAPPEAR WITHOUT PAYING; PROFITABLE CRIME IS LESS RISKY THAN
HOLDUPS, COPS NOTE.**

TEXT:

Rather than holding up high-tech companies at gunpoint, **thieves** are

discovering an easier way to **steal** computer chips, components and systems: open a phony business, order the products and disappear without paying.

Police and trade associations say the crime is an old scam adapted to **theft** of the newest technology. It has become a growing concern, with as many as 10...

... extremely valuable and easily resold," said Rich Bernes, who heads the FBI's anti-computer- **theft** squad in San Jose.

The basic pattern is simple: Con men rent an office, then...

... to order its products. Their credit references are companies that don't exist. When suppliers **check**, the **phone numbers** ring back to the con artists' own shop.

Occasionally, **swindlers** start with small, legitimate purchases to gain the company's trust. Eventually, they order a...

... sometimes, sales and marketing enthusiasm overwhelm vigilance," said Marylu Korkuch, a spokeswoman for the Technology **Theft** Prevention Foundation in New Jersey. "And that spells trouble."

No one has tracked how much of the estimated \$1 million Silicon Valley loses to high-tech **theft** each week is due to this scam. But police fear the number of cases will...

...cash.

Armed robbers face six years in prison plus possible enhancements, while those convicted of **fraud** may only face a year. There's a much greater chance of something going wrong...

... to report a violent crime than a scam. Add in those factors, officers say, and **computer**-related scams are **likely** to soar.

'A business decision'

"Basically, they (high-tech **thieves**) are making a business decision," said Keith Lowry, a San Jose officer specializing in computer ...

... additional 10 companies throughout the United States. They are awaiting trial on charges of grand **theft** and receiving stolen property.

While the case illustrates some common aspects of the scams, police say there are numerous variations.

Target smaller firms

Thieves typically target smaller businesses, expecting they wouldn't check credit references thoroughly, officers say. They...

... so overjoyed that they are landing a big order that they become careless.

Sometimes, the **swindlers** have hit several companies simultaneously for \$30,000 apiece. Other times, they have returned to...

...from checking their background thoroughly and to allow them to disappear

quickly.

Send someone to **check** out business **addresses** given for large orders. They may only be vacant offices or post office boxes - signs...

DESCRIPTORS: COMPUTER TECHNOLOGY **ROBBERY** COMPANY BUSINESS SAFETY ADVICE
Imex International ; Northwest Financial Savings ; Piiceon Inc ; San Jose ;
Technology **Theft** Prevention Foundation ; Tri Data Tech

12/3,K/5 (Item 1 from file: 624)

DIALOG(R)File 624:McGraw-Hill Publications

(c) 2005 McGraw-Hill Co. Inc. All rts. reserv.

00991225

**RICHARDSON ENDORSES BILLS IN CONGRESS TO CREDIT VOLUNTARY EMISSIONS
REDUCTIONS**

Utility Environment, Vol. 26, No. 3, Pg 1

January 15, 1999

JOURNAL CODE: UER

ISSN: 1503-9379

WORD COUNT: 753

TEXT:

... action on global warming. Waxman said he does not want companies to be able to ``**cheat** the system and future generations.''

GAO found four issues that should be **addressed** before awarding credit: **verification**, ownership, baselines and reporting levels. In looking at DOE's current programs for voluntary reductions...

... is the level of reporting, said GAO. ``Without company-wide reporting, it would not be **possible** to **determine** if a company's overall emissions were reduced,' ' it said.

et	Items	Description
S1	169294	FRAUD? OR DECEPTION? OR THEFT OR THIEV? OR LARCENY OR STEA- L? OR ROBBERY OR CHEAT? OR SWINDL? OR DISHONEST?
S2	2742303	CALCULAT? OR DETERMIN? OR COMPUT??? OR FIGURE??? OR ESTIMA- T? OR GAUG?
S3	1883041	POTENTIAL? OR LIKELIHOOD OR RELATIVE OR POSSIBL? OR PROBAB- LE OR PROBABILITY OR LIKELY
S4	1345437	CHECK??? OR COMPAR??? OR VERIFY? OR VERIFI? OR CONFIRM??? - OR VALIDAT? OR AFFIRM? OR CORROBORAT? OR AUTHENTICAT?
S5	813254	(PURCHASER? OR BUYER? OR SHOPPER? OR CONSUMER? OR CUSTOMER? OR USER?)(1W)(DATA OR INFO OR INFORMATION) OR SHIP()TO OR SH- IPPING OR BILL()TO OR ADDRESS? OR AREA()CODE? OR PHONE()NUMBE- R? OR ZIP
S6	1243747	RISK OR RISKS OR CHANCE OR SCORE
S7	74403	S2(4N)S3
S8	639	S7(S)S1
S9	8125	S4(4N)S5
S10	16	S8 AND S9
S11	12	S10 AND S6
S12	12	RD (unique items)
S13	4	S12 NOT PY>1999
File	15:ABI/Inform(R)	1971-2005/Oct 27 (c) 2005 ProQuest Info&Learning
File	610:Business Wire	1999-2005/Oct 27 (c) 2005 Business Wire.
File	810:Business Wire	1986-1999/Feb 28 (c) 1999 Business Wire
File	476:Financial Times Fulltext	1982-2005/Oct 27 (c) 2005 Financial Times Ltd

13/3,K/1 (Item 1 from file: 15)

DIALOG(R)File 15:ABI/Inform(R)

(c) 2005 ProQuest Info&Learning. All rts. reserv.

02495036 117543622

The manager's guide to internal control: diary of a control freak

Pickett, K H Spencer

Management Decision v37n2 PP: 93 1999

ISSN: 0025-1747 JRNL CODE: MGD

WORD COUNT: 90354

...TEXT: auditors are excellent. They have introduced value-added audits where they encourage us to adopt **risk** assessment, process reviews and a wider perspective of audits outside the old tick and check...

...well known model called The COSO model sees control as consisting of monitoring, control activities, **risk** assessment, control environment and information and communication. What I am looking for, is a model...top management, protect assets, promote compliance, secure value for money, be in line with defined **risk** criteria and so on and so forth... The problem is that this list does not...

...having an aim, making sure you have the means to achieve it and managing those **risks** that can impair your ability to get there. It is a driving force that moves...ahead at work but we must try to avoid pitfalls - but there is always some **risk** involved. This was well put by Blake and Mouton in their Management Grid (Figure 6...

...didn't bother and continued to view the scenery.

Jack continued "This is related to **risk** and views concerning the form that control takes. Let me take the concept of **risk** first..."

Bill finally took his cue to take part in some verbal sparring. He said; "Yes. My reading suggests that controls are directed towards areas that represent high **risk**. High **risks**, being the amount at **risk**, times the likelihood of this amount being lost or depleted (expressed as a percentage between...

...came up against the control problem. He went on; "We then establish the type of **risks** that may mean control objectives would not be achieved, say for example pressure selling, and control mechanisms. **Risk** then drives controls and in this way real problems are dealt with."

"Excellent" Jack announced...

...model you have described means controls are located at point A. Here we tackle high **risk** areas that can be controlled through the use of sound control mechanisms. We may go...

...make sure these controls are being complied with. However, my view is that the entire **risk** management model implicit in the above diagram is in itself a key control over managing an organisation. The perceived **risk** rating as high or low should also be subject to control, as this will change...basic example, but segregation is essentially about not allowing one person to control an at-**risk** process (that is - it involves the movement of funds and goods) from start to finishI have put together a checklist setting out attributes, **risk** and best practice on each aspect of the MCS in Appendix A of the file...

...happened. I've seen it happen time and time again. In fact on one high **risk** audit, we asked the section manager if we could view his operational procedures - he said...not depend on ignoring staff who blatantly breach important procedures and place the organisation at **risk**. It is just that a positive environment is seen as better than a punitive one...position or negotiation which seeks a win-win result by resolving the conflict with compromises (**Figure 18**)."

"This brings out the multi-dimensional view of management action - that may not be...people want good procedures and they will devise and improve them if given half a **chance**. In fact, during the interviews, staff expressed a wish to be able to track cash...problem is dealing with the child in all of us where we shun responsibility and **risk** for fear of failure. If we are also charged with dealing with factors that we cannot control, then this makes it worse. We must build processes that incorporate **risk** and uncertainty and the innate human psyche that is wholly unpredictable. Quite a challenge? But...

...as this again hides from control when it cannot be achieved and assumes a zero- **risk** /no-change position that will in the end mean the business fails. If we view...privileges. The point being that motive and means is not enough, without being given a **chance** to defeat the systems and controls. A more cynical view of the three-component model...

...thought. The upside is that a little research may isolate the types of areas at **risk** and some of the signals that there could be problems - for example a payments clerk...you. Your systems of internal control are there to act as a safeguard against this **risk**. In fact if you talk to a typical manager about the goal of internal controls...happening in the first place. So we seek to install strong control over assets at **risk** and ensure they are protected. For example, we may require cheques over a certain value...the local manager and his/her staff, it's simply a question of understanding the **risks**, keeping in mind signs that not all is well and being able to take action...

...called 'flowchart' - this term is used to describe the task of documenting the process at **risk** and who does what. So as to gain an understanding of how the work and...we mean by assuming a judicial position."

"5Interview the employee and give him/her the **chance** to explain. When fraud is involved and the person is taking part in police enquiries...

...show concern where the employee is not being represented properly or has not had a **chance** to state their case. I sat on an appeals panel where the employee had not...arrived at the topic of ethics. This is part of the controls that ensure the **risk** of fraud is properly managed. I've seen many frauds in my time and as...protect the organisation from abuse is morally unacceptable. The organisation's assets are therefore at **risk**. An organisation that does not address this problem is suffering from moral muteness."

"I remember...for avoiding and/or exposing moral violations;
- That the whistleblower's action have some reasonable **chance** of success (Vinten, 1994)."

"This is a really tight model that means going public only...

...we will again be breaking our internal disciplinary code. The reality then, is that we **risk** dismissal - which is normally enough to put most

people off. It is very important that...

...can cope with whistleblowing - including:"

- Make sure employees understand company's codes of ethics;
- Use **risk** assessment to tackle key areas;
- Ensure employees do not face retaliation for speaking out;
- Discuss...on leaving large sums of cash on his desk at work. We pointed out the **risk** in this to which he replied - 'If I can't trust my staff; who can...

...understanding the systems and how they can be beaten;"

- "opportunity - if we allow people the **chance** to abuse systems then there is always the **risk** that they will. If they pass up these opportunities today, this does not mean they...is some sensitivity. It may be used to deal with matters such as staff secondments, **risk** ratings, supplier selection, assignment of resources and so on. In this way everything can be...

...as such. Clear and firm controls need to be in place to combat the real **risk** of fraud. A story from Boswell (Life of Samuel Johnson) will help consolidate this view...two now. I want to include financial systems because they tend to hold a high **risk** rating. "

Flicking on the dictaphone Jack announced, "Let's make a start."

Information systems

"I...also need to be involved in contingency planning if we have a role in high- **risk** databases. One control that has a main role in IT security is related to the...18 Ensure that remote access requests are subject to call-back so that the terminal **address** can be **verified** before we accept the password.

19 Be careful about establishing password patterns. Some networks do...subject when dealing with internal controls. This is because they tend to attract a high **risk** rating when assessing the extent to which we need to ensure they are well controlled...

...financial accounts have to be prepared, audited and filed for public record."

"Going back to **risk** . One version of this is the amount of assets and interests at **risk** , times the likelihood that they will be eroded or lost. The resulting figure will indicate...

...be audited. Even here audit will look at matters that it perceives to hold high **risk** , and only to the ...time. There is no short cut to management assessing its financial systems, understanding the inherent **risks** and establishing suitable arrangements for managing these **risks** ."

"There are several key issues to consider when discussing financial systems:"

"1 Ownership - Management must...always work out as implied by the following press release:"

Families are being put at **risk** by some supermarkets and butchers selling frozen meat as 'fresh'... (Daily Mail, 1996i)."

"Having said...

...few seconds, each time with a large fish, Bill looked more relaxed.

"This may be **cheating** but so be it. I want fish and now I've got them." suggested Bill...

...Bill, we have really finished our work on internal control. We have discussed definitions, procedures, **fraud**, information systems, financial systems, quality and value for money. That is really all there is. ...are dealt with and employees feel committed and competent, then we have a much better **chance** of success. Getting people to release their creative energies is not easy. At first sight the occasional gamble and manage corporate **risk** properly. At the end we lose this accountability by seeking it too rigidly. We take...Jack announced that he would have to set about preparing lunch. This gave Bill the **chance** to spend some time with Ruth who came out after talking with Jack's wife...systems of control to ensure policy frameworks are adhered to, and assets are protected from **fraud**, information systems work, and quality products are delivered. This should not be a matter of...

13/3,K/2 (Item 2 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2005 ProQuest Info&Learning. All rts. reserv.

01990895 50464080

Flaming, complaining, abstaining: How online users respond to privacy concerns

Sheehan, Kim Bartel; Hoy, Mariea Grubbs
Journal of Advertising v28n3 PP: 37-51 Fall 1999
ISSN: 0091-3367 JRNL CODE: JOA
WORD COUNT: 9507

...TEXT: fall under Keaveney's (1995) category of "ethical problems." Ethical problems include activities seen as **dishonest**, intimidating, unsafe, unhealthy or which represent conflicts of interests. Given Andreason and Best's (1977...

...is fair game for others to see and hear. In contrast, privacy problems are more **likely** to emerge for nonpublic **figures** unaware of the possibility that they are being observed, even in public situations. At the ...situations described in Table 1. The total concern scores ranged from 15 to 105. A **score** of 15 would represent an individual for whom none of the situations caused concern with privacy. A **score** of 105 would represent an individual for whom every situation caused extreme concern with privacy. The mean total concern **score** was 58.86, with a standard deviation of 18.93. Cronbach's Alpha, an estimate of internal consistency, was .92. The total concern **score** was correlated with each of the seven behaviors to determine if a relationship existed between...about half of all unsolicited e-mail that they receive (mean=3.53). The mean **score** and total sum correlation coefficient is -0.07806. The negative coefficient suggests that as privacy...

...reported they rarely notify their ISPs about unsolicited e-mail (mean=1.76). The mean **score** correlated with the total concern **score** resulted in a Pearson Correlation Coefficient of .2784 1. The correlation is significant (p=.0001...

...average was providing incomplete information when registering for web sites (mean=3.65). This mean **score** suggests that individuals are adopting that specific behavior during less than half of their online...to send a "flame," will result in their names being placed on a list of **confirmed** "good" e-mail **addresses**, which would result in the receipt of even more e-mail. Avoidance behaviors are perhaps...that the topic line must be compelling, persuasive and believable in order to maximize the **chance** of the e-mail being opened. Online advertisers, then, must focus on creating email messages...

13/3,K/3 (Item 3 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2005 ProQuest Info&Learning. All rts. reserv.

01799647 04-50638

Betting on the Net: An analysis of the government's role in addressing Internet gambling

Kish, Stevie A

Federal Communications Law Journal v51n2 PP: 449-466 Mar 1999

ISSN: 0163-7606 JRNL CODE: FCL

WORD COUNT: 7264

...TEXT: years: uneasiness about the morality of the activity; the likelihood of addiction; the possibility of **fraud**; and the conflict between state versus national regulation.23 Questions of morality primarily surface in...

...reminiscent of arguments made during the passage of the Communications Decency Act. Because children have **potentially** unlimited access to **computers** and the Internet, it is possible that without proper monitoring they will access gambling Web...gambling. Also, all Internet gamblers could be required to submit biographical information such as age, **phone number**, and **address**. Upon **verification** of this information by the gambling Web site operator, the Internet gambler would be issued...Crow Dog and Oliphant Fistfight at the Tribal Casino: Political Power, Storytelling, and Games of **Chance**, 29 ARIZ. ST. L.J. 171, 178 (1997) (quoting COMMISSION ON THE REVIEW OF THE...

13/3,K/4 (Item 4 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2005 ProQuest Info&Learning. All rts. reserv.

01696771 03-47761

Avoiding credit fraud with due diligence

Kerins, James

Business Credit v100n8 PP: 17, 19 Sep 1998

ISSN: 0897-0181 JRNL CODE: CFM

WORD COUNT: 1254

ABSTRACT: Most business owners and credit managers understand that an element of **risk** is part of any business transaction. Preventing credit **fraud** requires a thorough program of credit due diligence during the beginning phases of the business relationship. To counteract the vast **potential** for **fraud** created by **computers**, credit managers need to train their personnel in reviewing and analyzing all the different documents...

...TEXT: reach of computer technology.

Most business owners and credit managers understand that an element of **risk** is part of any business transaction. But how can the diligent credit manager prevent fraud before it happens-or, at least, minimize all the **risks** that it will? The best answer lies in undertaking a thorough program of credit due...

...longer good business practice to accept officiallooking documentation at face value. To counteract the vast **potential** for **fraud** created by **computers**, credit managers need to train their personnel in reviewing and analyzing all the different documents...

...that applies, regardless: the level of verified detail should be consistent with the level of **risk** associated with the transaction. The greater the **risk**, the more detailed the verification process should be.

In addition, it is critical to make...

...a range of commercially available databases. Sophisticated users of these databases will be able to **gauge potential risk** in a matter of minutes. But with the analysis of data in which there are...
...about.

The next stage of preventing credit fraud falls under the rubric of minimizing the **risks**. Here the diligent credit manager will want to address the **risks** inherent in the delivery of the product-from the potential fraudsters' perspective. "Product diversion" or...

...a thriving business for fraudsters. An appropriate level of due diligence on the "ship to" **address** should supplement all previous **verification** efforts. Here is a brief list of the basic searches that should be made to **verify** the legitimacy of the **shipping address**: **address check**, **phone number -to- address cross check**, **phone number -to-company name cross check**, surrounding businesses check, and the property ownership/square footage check.

This checklist of searches can...

...address to uncover corporate affiliations, if such exist. The latter plays a role in minimizing **risk** because a favorite fraudster ploy is to establish multiple business identities at various addresses or...

...be less than desirable. Clearly, the disparity invites further investigation.

The final stage of minimizing **risk** occurs during the ongoing relationship with the business given credit and/or that business' payment...corporations and subsidiaries with manufactured credit references. But the formula for avoiding or minimizing the **risk** of these schemes remains the same, regardless of the level of complexity involved. Proactive rather...

Set	Items	Description
S1	169294	FRAUD? OR DECEPTION? OR THEFT OR THIEV? OR LARCENY OR STEA- L? OR ROBBERY OR CHEAT? OR SWINDL? OR DISHONEST?
S2	2742303	CALCULAT? OR DETERMIN? OR COMPUT??? OR FIGURE??? OR ESTIMA- T? OR GAUG?
S3	1883041	POTENTIAL? OR LIKELIHOOD OR RELATIVE OR POSSIBL? OR PROBAB- LE OR PROBABILITY OR LIKELY
S4	1345437	CHECK??? OR COMPAR??? OR VERIFY? OR VERIFI? OR CONFIRM??? - OR VALIDAT? OR AFFIRM? OR CORROBORAT? OR AUTHENTICAT?
S5	813254	(PURCHASER? OR BUYER? OR SHOPPER? OR CONSUMER? OR CUSTOMER? OR USER?)(1W)(DATA OR INFO OR INFORMATION) OR SHIP()TO OR SH- IPPING OR BILL()TO OR ADDRESS? OR AREA()CODE? OR PHONE()NUMBE- R? OR ZIP
S6	1243747	RISK OR RISKS OR CHANCE OR SCORE
S7	74403	S2(4N)S3
S8	639	S7(S)S1
S9	8125	S4(4N)S5
S10	16	S8 AND S9
S11	12	S10 AND S6
S12	12	RD (unique items)
S13	4	S12 NOT PY>1999
S14	133531	DETECT???
S15	7072	S14(3N)S1
S16	1761277	NON()PERSONAL OR NONPERSONAL OR ELECTRONIC OR ON()LINE OR - ONLINE OR INTERNET OR DIGITAL?
S17	3359520	TRANSACTION? OR SALE? OR COMMERCE OR SHOP? OR RETAIL? OR - SELLING OR PURCHAS? OR MARKETING
S18	239450	S16(2W)S17
S19	928	S15 AND S18
S20	36	S19 AND S7
S21	103	S19 AND (S7 OR S9)
S22	23	S21 NOT PY>1999
S23	23	RD (unique items)
File	15:ABI/Inform(R)	1971-2005/Oct 27
	(c)	2005 ProQuest Info&Learning
File	610:Business Wire	1999-2005/Oct 27
	(c)	2005 Business Wire.
File	810:Business Wire	1986-1999/Feb 28
	(c)	1999 Business Wire
File	476:Financial Times Fulltext	1982-2005/Oct 27
	(c)	2005 Financial Times Ltd

23/3,K/1 (Item 1 from file: 15)

DIALOG(R)File 15:ABI/Inform(R)

(c) 2005 ProQuest Info&Learning. All rts. reserv.

02556276 254348901

Fraud auditing

Vanasco, Rocco R

Managerial Auditing Journal v13n1 PP: 4-71 1998

ISSN: 0268-6902 JRNL CODE: MAJ

WORD COUNT: 49489

...ABSTRACT: associations, governmental agencies, and international accounting and auditing bodies in promulgating standards to deter and **detect fraud**, domestically and abroad. Specifically, it focuses on the role played by the US Securities and...

...TEXT: associations, governmental agencies, and international accounting and auditing bodies in promulgating standards to deter and **detect fraud**, domestically and abroad. Specifically, it focuses on the role played by the US Securities and...

...that the problems facing the auditing profession today may stem from the ostensible obsession with **fraud detection** shown by some Victorian era practitioners. This obsession created an expectation gap among the public. Emphasizing **fraud detection** as the primary audit objective lasted until the 1930s, when the principal audit objective became...

...Spicer and Pegler's Practical Auditing, the principal reason for instituting an audit are to **detect fraud** and errors. Walker (1993) observed that auditors have become less interested in **detecting fraud**. There is evidence that auditors do not regard the reporting of significant audit observations to...

...no responsibility for the audited financial statements. In general they are not overly concerned with **detecting fraud** and errors.

In the late 1940s, the external auditors did not assume a direct responsibility for fraud because of their inability to **detect fraud** involving unrecorded transactions, theft, and other irregularities. This was done to shield accounting firms from...Auditors must investigate if they suspect fraud; but in this case, the former management made **fraud** difficult to **detect** because two executives turned the company "into an engine of theft against outsiders."

In 1984...fraud case is simple; although the contract does not call for an audit examination or **detection of fraud**, auditors should be responsible for disclosing circumstances causing them to believe fraud exists.

In the...drastically over the years. In the early 1900s, the external auditors' primary responsibility was the **detection of fraud** because audits were primarily involved with cash transactions.

In 1936, the American Institute of Accountants...

...No. 1, Codification of Auditing Standards and Procedures in 1972.

The auditor acknowledged responsibility for **detecting fraud** that would normally be uncovered by an examination performed in accordance with GAAS:

The responsibility of the independent auditor to **detect fraud** (which responsibility differs as to clients and others) arises only when such

failures clearly result...

...cost would be prohibitive. Even then he could not give assurance that all types of **fraud** had been **detected** or that none had existed because of items such as unrecorded transactions, forgeries, and collusive...1967 which was superseded by SAS No. 1. It dealt with the auditors' responsibility for **detecting fraud**. The auditor is required to look specifically for irregularities which may have a material effect...

...enterprise related factors;

* accounting practices; and

* uncertainty

It seems that the auditor's responsibility to **detect** management **fraud** depends on the manner in which it was perpetrated, its pervasiveness, and the likelihood of...be if: SAS No. 53 changed the way auditors conducted audits so that they actually **detected** more **frauds**; or changed user expectations about what auditors are supposed to do. He believes that SAS ...
...statements."

In 1991, Congressmen Ron Wyden, Edward J. Markey, and John D. Dingell felt that **fraud detection** should be one of the primary goals of any audit of financial statements. They introduced HR 4313, "Financial **Fraud Detection** and Disclosure Act," which represents an attempt to put more pressure on independent auditors to **detect fraud**. In March 1993, the AICPA announced its endorsement of HR 574, the Financial **Fraud Detection** and Disclosure Act (the Wyden Act), on the basis that it should bolster public confidence...recommendation of the Public Oversight Board and proposed several accounting reforms in order to improve **fraud detection**, strengthen auditor independence, and other related auditing issues. This was done in response to some...

...improve the climate for tort reform by expanding auditors' effort to:

* improve the prevention and **detection** of **fraud**;

* enhance the utility of financial reporting to those who rely on it;

* assure the independence...

...alleged accounting failures (Miller, 1993). The board of directors also endorsed the proposed federal "Financial **Fraud Detection** and Disclosure Act" and stressed that auditors should receive a stronger support from management to allow them to prevent and **detect fraud**:

Every participant in the financial reporting process has a stake in preventing wrongdoing and all...related to consideration of fraud in an audit." The better our profession can become in **detecting fraud**, the better we will serve the public interest and increase the value of our services...

...to occur.

The standards do not, however, specify that internal auditors are responsible for the **detection** of **fraud**. Internal auditors must be alert and consider the possibility of fraud when carrying out an...

...for fraud. The SIAS added several subsections to Standard 280 to address

the issue of **fraud detection** .

In 1986, The Institute of Internal Auditors took a stand on internal audit involvement in...

...financial reporting, and issued a paper entitled The Role of Internal Auditors in the Deterrence, **Detection** , and Reporting of **Fraudulent** Financial Reporting (Institute of Internal Auditors, 1986). The paper was prepared for the National Commission of Fraudulent Financial Reporting.

The pervasive influence by the Institute of Internal Auditors to deter, **detect** , and report **fraud** will be discussed in the following sections.

The role of the association of certified fraud...

...white-collar fraud program to accredit as Certified Fraud Examiners (CFEs) people with skills necessary to **detect** , investigate, and deter **fraud** . CFEs often have accounting or auditing backgrounds and work in such fields as forensic accounting...1982).

The Institute of Management Accountants' (IMA) research report The Role of Analytical Procedures in **Detecting** Management **Fraud** addresses the need to improve the auditor's ability to **detect** management **fraud** with a better knowledge of analytical procedures (Freedman, 1993).

The IMA believes that management and the board of directors should establish an internal control structure to prevent or **detect fraud** . Part of that structure is the control environment. Factors in that environment are:

- * management philosophy...

- ...independent public accountants that:

- * auditing standards be changed to recognize the auditor's responsibility for **detecting fraudulent** financial reporting better; and

- * the auditor's standard report be improved to better communicate the... systems based on the fundamental principles of good internal control be established and used.

- * To **detect** and investigate **fraud** , organizations must ensure the existence of strong internal audit departments with sufficient resources to pursue...

- ...may be required by responsible members of the organization.

- * Help evaluate the extent to which **fraud** prevention and **detection** are given fair consideration along with other operational activities.

- * Seek directly or indirectly to achieve...

- ...be a consensus that auditors need to sharpen their skills in identifying red flags in **detecting fraud** . Thompson (1991) views the internal auditor role with regard to fraud as identifiers, investigators, resident ...people being not held responsible for their actions; and

- * inadequate training for those responsible for **fraud** prevention/**detection** .

The most often reported "red flags" are:

- * weaknesses in internal control;
- * ignoring audit reports;
- * inventory...

...misconduct in nonprofit organizations have drawn attention to the role of the auditor in the **detection** of **fraud**. Nonprofit organizations must gain a better understanding of what an audit is designed to achieve...
...of bank directors, security personnel, audits, and examiners of financial institutions is the deterrence and **detection** of **fraud**. Gup (1994) observed that banks have learned the hard way how to protect themselves against...

...item processors. The method of detection identified in the event or factors that triggered the **detection** of **fraud** were:

- * internal controls;
- * routine audits;
- * customer complaint/inquiry;
- * accident, tip-off, unusual activity of perpetrators...bank fraud. He added that "banks' independent auditors should report to the bank when they **detect** **fraud**. If they resign from the account, they should report the reasons to regulators" (FDIC, 1986...from 1990 through 1992. As fraud abuse levels rise, insurers are calling for software to **detect** billing aberrations, **fraud**, and abuse in health care claims (Friedman, 1994).

The 1994 Department of Health and Human...
...claim data to examine the billing and medical activities of health care providers to help **determine** the most **likely** abusers ("Cigna-Healthcare," 1994).

Gardner (1995) reports that the Department of Justice and other federal...
...replaced him.

From the lessons learned from the above cases, Stohl drew the following conclusions:

- * **Fraud** **detection** lies in the detail.
- * Follow-up is critical.
- * Suspected wrongdoing should be fully investigated to...combat it with great fervor. As Louisiana Insurance Commissioner, he increased manpower and budget for **fraud** **detection** and financial auditing in 1992. He improved his department's link with federal investigators and encouraged state legislators to pass laws making it easier to **detect** and prosecute insider **fraud**.
The results are impressive: 32 insurance executives in Louisiana were convicted of various white-collar...companies had no written fraud policy
- * Over three-fourths of those surveyed believed that the **fraud** they **detected** could have been avoided.
- * Over three-fourths of **fraud** **detected** was committed by the companies' own staff.

* More than a quarter of the companies suffered...

...audit budget is always below the adequacy for any effective audit planning. Under these circumstances, **fraud detection** may be the last priority.

Nnanna (1995) reported that fax fraud in Nigeria is rampant...with the same level of assurance, whereas most auditors would agree that they cannot possibly **detect** misstatements arising from **fraud** or illegal acts with the same level of assurance that they can detect misstatements arising... can be bridged." The report asserts that the profession needs to embrace the role of **detecting fraud**, widen its responsibility beyond the shareholders as a group, and spin off its audit regulatory...
...the questions of how much responsibility auditors and management must take when it comes to **detecting** and reporting **fraud** and illegal acts. The exposure draft would require auditors to assess the risk that fraud...

...statements require auditors to design audit procedures so as to have a reasonable expectation of **detecting** misstatements arising from **fraud** or error that are material to the financial statements. Some believe that the cost of...accounting and financial functions.

The value of internal control is apparent in both preventing and **detecting fraud**. In a recent survey conducted by Welch et al. (1996) shows that the majority of...

...the symptoms of fraud, the red flags or indicators exist to alert management of wrongdoing.

Fraud detection

In planning tests for a fraud audit, the goal is often to test an unrepresentative...

...1, Extension of Auditing Procedures (1939) stressed that the external auditor is not responsible for **detecting fraud** in the ordinary examination of the financial statements:

In making the ordinary examination, the independent...by management, tests conducted by auditors and other sources both within and outside the organization. **Detection of fraud** consists of identifying the indicators of fraud sufficient to warrant recommending an investigation. The internal auditing department's responsibilities for **detecting fraud** when conducting audit assignments are to:

* Have sufficient knowledge of the indicators of fraud.

* Be...

...to opportunities such as control weaknesses that could allow fraud.

* Conduct additional tests directed toward **detection of fraud** if significant weaknesses are found.

* Evaluate the indicators and decide whether further action is necessary...

...statement of management's commitment to corporate ethics. Internal auditors would be more likely to **detect fraud** if they develop their ability to recognize and question changes that occur in

organizations. Examples of audit tests to **detect fraud** are:

To **detect** the alteration of the beginning balance in the monthly checking account reconciliation, the auditor should...

...agencies is to verify new vendor firms listed in a professional association catalog and/or **verify** the vendor name and **address** through the telephone book.

* The means of detecting alteration of receipts for employee expenses is...
...themselves to commit an irregularity.

Thompson (1991) offers some good reasons why auditors do not **detect fraud**. The assumption is that they:

- * do not believe that detection is their job,
- * are too...
...occurrence,
- * fail to follow through on symptoms of fraud,
- * are concerned about career implications of **fraud detection**.

Matsumura and Tucker (1992) conducted a study of the interaction between a manager and an auditor which resulted in an increase in **fraud detection**. In the game, the manager chose a probability of committing fraud whereas the auditor decided...

...were examined to assess their effects on tests of transactions and detailed tests of balances, **fraud detection**, and incidence of **fraud**. Increasingly the auditor's penalty was found to decrease **fraud** and increase **fraud detection**.

Thompson (1992) suggests a five-step approach for **fraud detection**:

- 1 Know **fraud** exposure in specific terms.
- 2 Know exposure specific symptoms of fraud.
- 3 Be alert for...

...Ziegenfuss' survey (1996) of municipal and local governments shows that the most effective tools for **fraud detection** are:

- * internal audit review;
- * specific investigation by management;
- * employee notification; and
- * accidental discovery.

According to the deputy director of UK's Serious Fraud Office, the reasons why auditors fail to **detect fraud** are:

- * inadequate scope of auditing testing and inquiries;
- * restrictions of auditors' work by management;

- * auditors...internal auditor's procedures lend to suspicion of some kind of wrongdoing, the auditor should:
- * **determine** the **possible** effects of the wrongdoing;
- * discuss the matter with the appropriate level of management; and
- * decide...on the following assumptions:
- * the independent auditor is currently facing unprecedented liability for failing to **detect** material **frauds** ;
- * the **detection** of these **frauds** by independent auditors is difficult at best, even with adequate training, and
- * the auditor's primary concern should be prevention, not **detection** .

The **fraud** prevention program should have three realistic and measurable goals:

- 1 reduce losses resulting from fraud;
- 2 deter fraud through proactive policies; and
- 3 increase the likelihood of early **fraud detection** .

Albrecht (1996a) agrees with chairman Wells that "fraud prevention is far more cost-effective than **fraud detection** " but for the external auditors "activities such as client acceptance and fraud prevention aren't...

...believable (Albrecht, 1996a).

Analytical auditing procedures, including horizontal and trend analysis, are important and effective **fraud detection** techniques. By analyzing sales in the last three or five years, auditors can detect unexpected... irregularities is high. According to the National Commission on Fraudulent Financial Reporting, the potential for **detecting fraudulent** financial reporting through analytical auditing procedures has not been fully realized. The Report points out...

...number of cases reviewed by the Commission, analytical procedures might have increased the likelihood of **detecting fraudulent** financial reporting (PSB 89-2).

Albrecht (1996a) noted that analytical fraud symptoms include transactions or...

...conspiring with another company's purchasing agent to inflate sales. Trend and ratio analysis may **detect** potential **fraud** such as:

- * An unexplained increase in the default rate caused by bogus loans.
- * An extraordinary...

...effective they are as a control (Wallace, 1995).

Bank reconciliations play a powerful role in **detecting** potential **fraud** by employees. The IIA Houston Chapter (1993) reported that an internal auditor noticed that one...Louis provides white-collar crime information on embezzlement and environmental crimes committed in the city.

- * **Fraud Detection** Kit offers instructional materials to help businessmen

detect and deduce occurrences of fraud within their...conduct is by not hiring dishonest employees (Sawyer, 1988).

Kroll Associates Inc. (1993), a business **fraud detective** agency based in New York City, offers the following list of behavior and events as...

...audit tests are not designed to make detailed examinations and verifications of all transactions to **detect** employee **fraud** and other irregularities. However, internal auditors have the basic responsibility to use due professional care...to:

- * keep bank and book amounts in agreement so that a bank reconciliation will not **detect** the **fraud** ;

- * correct the customer's account within a few days. Any discrepancy in the customer's...

...invoices; and

2 increased sale prices substantially above the company's list prices.

Auditors can **detect** such a **fraud** while performing sale cutoff tests and examining transactions a few days ...do not make sense.

- * Dumpster diving can sometimes prove to be a useful tool in **detecting fraud** .

- * When **fraud** is suspected, even the slightest variation from the norm is worth pursuing.

- * It helps to...ghost employees;

- * failing to delete employees who have been terminated; and

- * submitting excessive overtime.

To **detect** these kinds of **fraud** , auditors apply the following analytical tests:

- * duplicate and validity tests;

- * exception testing; and

- * recalculations (Crowder...to have large inventory shrink, may indirectly encourage fraud in the inventory areas.

- * Means of **detection** of **fraud** are often suspicions by fellow employees or excessive greed that prompts an investigation.

In 1978...

...of a cost-effective fraud auditing program based on audit hooks or red flags to **detect fraud** . The hooks are embedded during the design phase of a data processing system. For an insurance company the audit hooks are designed to **detect** unauthorized and potentially **fraudulent** charges to policyholders.

Menkus (1990) observed that understanding how computer fraud can occur will not...indicated that the organizations placed specific responsibility on the internal audit department for prevention and **detection** of computer **fraud** . The study also indicated that 96 percent of internal auditors

consider the possibility of fraud...

...Crumbley (1991), in *Trap Doors and Trojan Horses*, introduced new auditing techniques to prevent and **detect fraud**.

The following surveys show that computer frauds are mostly attributed to the inadequacy or lack...

...new technologies are becoming more widely used. In 1996, Mastercard and Visa International developed Secure **Electronic Transactions (SET)**, a new standard for credit card payments in the Internet. The key to SET... internal auditor's procedures lead to suspicion of some kind of wrongdoing, the auditor should **determine** the **possible** effects of wrongdoing, discuss the matter with the appropriate level of management, and decide with...process may be imperiled (Wallace, 1995).

In 1993, the US Congress proposed a bill "Financial **Fraud Detection** and Disclosure Act." It aims to force auditors to report misleading corporate financial accounting to...to increased employee fraud and opens the door for more management abuses.

Conflict of Interest **fraud**

The primary **detective** control against selfdealing is to match the employee master file records against the vendor file...

...reoccurrence of this type of problem, a more effective vendor-selection process was established.

To **detect** conflict of interest **fraud**, Kramer (1996) suggests several steps including the test for indicators:

- * improper sole source awards;
- * low-bid award;
- * multiple purchases under bid limit.

Crowder (1997) also lists several procedures to **detect** potential **fraud** arising from employee conflict of interest. Auditors use CATTs which allow to **compare**:

- * vendor **addresses** to employee **address**;
- * vendor address to employees' outside business addresses; and vendor telephone numbers to employees' home telephone...

...irregularities have spearheaded several court rulings and shaped the auditing standards.

Leading writers list the **detection** of **fraud** as one of the most important purposes of auditing. They view auditing as an important...

...titled "Expectation gap can be bridged" and urged the profession to embrace the role of **detecting fraud**. Also in Canada, an expectation gap exists since users of financial statements believe that auditors...recent changes in the business environment, the result being that it is easy to perpetrate **fraud** without being **detected** by auditors. This is because traditional auditing is conducted in a vacuum, with no link...

...the industry sector, the IIA could establish task forces to develop

"industry guides" dealing with **fraud** prevention, **detection**, deterrence, and reporting. There seems to be a consensus that both internal auditors and external auditors need to sharpen their skills to meet the challenges of **fraud detection** and prevention.

23/3,K/2 (Item 2 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2005 ProQuest Info&Learning. All rts. reserv.

02325237 86065977

The internal auditor as fraud-buster

Hillison, William; Pacini, Carl; Sinason, David
Managerial Auditing Journal v14n7 PP: 351-362 1999
ISSN: 0268-6902 JRNL CODE: MAJ
WORD COUNT: 6719

...ABSTRACT: alike. Most accounting practitioners realize and acknowledge that external auditors are often not positioned to **detect** the occurrence of **fraud**. External auditors lack the continuous presence necessary for the establishment and implementation of fraud prevention...

...TEXT: percent of investors expected absolute assurance that material misstatements in the financial statements owing to **fraud** would be **detected** (Epstein and Geiger, 1994). The auditing profession has been criticized for both failing to **detect fraud** and failing to report fraud once discovered. It has been reported that independent auditors detect...

...countries have concluded that financial statement users believe independent auditors have a greater responsibility for **detecting** and reporting **fraud** and/or financial misinformation than was being met (Porter, 1996). These bodies include:

- National Commission...

...acts.

Most accounting practitioners realize and acknowledge that external auditors are often not positioned to **detect** the occurrence of **fraud**. External auditors lack the continuous presence necessary for the establishment and implementation of fraud prevention...

...perpetrators. This raises the question: "Who in an organization is in the best position to **detect** and prevent **fraud**?", particularly asset misappropriation. Such a query takes on added importance when one considers that more firms in 1998, compared to 1994, cite an insufficient emphasis on **fraud** prevention and **detection** as contributing to a rise in fraud (KPMG Peat Marwick, 1998). This article focuses on to prevent, deter, **detect**, and report **fraud**.

The fraud-buster role of internal auditors

The implementation of both SAS No. 82 and...losses. This indicates that internal auditors should focus their efforts on the prevention, deterrence, and **detection** of **fraud** involving cash, but many other of the balance sheet assets are at risk. In some...

...waiting for situations to be brought to the forefront. A proactive stance on preventing and **detecting fraud** should increase employee perception of the likelihood of detection. In addition to being aware of... and a trade supplier or conspiracy among two or more vendors.

This type of contract **fraud** might be **detected** by analyzing contract files for the same contractor routinely bidding last, bidding lowest, or obtaining...

...what assets are held and how they could be misappropriated. For those organizations involved in **electronic commerce**, a threat analysis should also involve an assessment of exposure to employee misappropriation or destruction...

...to highlight the most vulnerable assets. The analysis is viewed as a proactive step in **fraud** prevention and **detection**. Consideration of each class of asset and the evaluation of the exposure to loss helps...

...a fraud hotline.

An employee fraud hotline is the single most cost-effective means for **detecting** occupational **fraud** and abuse (ACFE, 1996). A hot-line is simply a special telephone number that a...retina patterns, and digital signatures. The latter is a common type of control used in **electronic commerce transactions** (for example, it helps authenticate a purchasing cardholder and a merchant). New forms of password...

...invasion by unauthorized employees or other parties. Also at stake is the security of all **electronic commerce** conducted via Web sites. One control that addresses this problem is encryption. Any process of...will also reveal what additional steps, if any, internal auditors can take to reduce the **likelihood** of **computer fraud**.

9. Surprise fraud audits

As an overall consideration, surprise pre-emptive fraud audits should...

...today.

Conclusion

Much attention has been paid to the role of the independent auditor in **detecting fraud**, but internal auditors are in the best position to prevent, deter, and **detect fraud**. The implementation of SAS No. 82 and the passage of the Private Securities Litigation Reform...

23/3,K/3 (Item 3 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2005 ProQuest Info&Learning. All rts. reserv.

01854847 05-05839

E-commerce--the way to go

Mandell, Mel

World Trade v12n8 PP: 31 Aug 1999

ISSN: 1054-8637 JRNL CODE: WLD

WORD COUNT: 757

DESCRIPTORS: **Electronic commerce** ;

ABSTRACT: Over one trillion dollars in **electronic commerce** in 4 years is projected by one market research outfit. Primus Telecommunications Group Inc. chose...

...TEXT: on the forms ranged as high as 15%. There was also no easy way to **detect fraudulent** orders, a big, profit-eating headache for the telecommunications industry. And the entire process from...

...a 70% reduction in errors because of all the built-in checks, such as instant **checking** of **area codes** and postal codes against a big database. Next, completed orders go directly to the Internet...

...It now takes only one week from order-taking to connection. POEMS also includes a **fraud - detection** module based on that database of area codes and corresponding postal codes. In other words...

23/3,K/4 (Item 4 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2005 ProQuest Info&Learning. All rts. reserv.

01837769 04-88760

Card fraud: Down but not out

Punch, Linda

Credit Card Management v12n3 PP: 30-42 Jun 1999

ISSN: 0896-9329 JRNL CODE: CCM

WORD COUNT: 3096

...ABSTRACT: dynamics of the industry. The anonymity offered by the Internet and the rapid growth of **electronic commerce** have opened a whole new venue for card fraud. ...

...TEXT: of marketing for Providence, R.I.-based Nestor Financial Solutions, a developer of neural-network **fraud - detection** products. "When you get complacent is when you get hit hard."

While fraud losses may...

...dynamics of the industry. The anonymity offered by the Internet and the rapid growth of **electronic commerce** have opened a whole new venue for card fraud. A criminal placing orders online with...millions of dollars," says Lisker.

Compounding the problems of fighting fraud is the growth in **electronic commerce**. The Internet provides a layer of protection for criminals because it allows them to commit...will hold them liable for losses if they fail to get a cardholder signature or **verify** the **shipping address** before delivering the product or service, Whatley says. As an example he cites an incident...

...shipped before the merchant realized the account number was fraudulent. Because the merchant failed to **verify** the **address**, he had to bear the loss.

And there was little help from law enforcement because...offer similar products for screening for fraud.

Implementation of Visa's and MasterCard's Secure **Electronic Transactions** protocol, digital certificates which authenticate the legitimacy of both the merchant and the cardholder, and other systems also are expected to cut fraud losses in **electronic commerce**. However, many of those are between 18 months and 24 months of being rolled out, Nestor's Spillane says.

But even the most sophisticated **fraud detection** and prevention systems can fail if not used properly, says Whatley, who notes that many...

23/3,K/5 (Item 5 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

(c) 2005 ProQuest Info&Learning. All rts. reserv.

01806668 04-57659

On-line security, payment services aid e-tailers stung by fraud

Corral, Cecile B

Discount Store News v38n8 PP: 20-25 Apr 19, 1999

ISSN: 0012-3587 JRNL CODE: DSN

WORD COUNT: 1053

DESCRIPTORS: **Electronic commerce** ;

ABSTRACT: As much as 5% to 6% of the average **Internet retailer's transactions** involve consumer fraud, according to figures recorded by CyberSource, a developer of software systems that **detects** online fraud. An e-mail address will not reveal a customer's identity or location, let alone...

...TEXT: is most often portrayed as the victim. But less is said about the thousands of **on - line retailers** that unknowingly conduct transactions with illegitimate consumersthe kind who drain profits through extensive use of...

...truth, consumer cyber fraud runs rampant. As much as 5% to 6% of the average **Internet retailer's transactions** involve consumer fraud, according to figures recorded by CyberSource, a developer of software systems that **detect** on line **fraud**. What's more, its assessments for Web businesses selling software and other digital goods are much worse; they show that 30% of total **Internet sales** result in attempted credit card fraud.

What's a retailer to do? Tracking the identity...

...the purchases, though, Langenderfer said ecommerce merchants face two potential problems when they accept any **on - line credit card transaction** :

* A higher processing rate than bricks-and-mortar retailers. Credit card companies consider the fraud...
...fraudulent transactions.

(Illustration Omitted)

Captioned as: Cybersource (top) is a developer of software systems that **detect** on-line **fraud**. Paymentech (above) provides credit card processing for retailers, some of which include America Online and...

...from such fraudulent transactions because the risks are too high," said John Shirey of the **electronic commerce** division at Paymentech, a Dallasbased company that provides credit card processing for retailers. Some of...

...by [accepting them] you run some major risks."

The Lanfords, also the founders of the **on - line marketing** service Netrageous.com, set up Scambusters.com after they got stung by a Web shopper...

...merchants to accurately verify credit card information recorded on line. They include systems such as " **address verification** services," which call on pin numbers and biometrics-fingerprint authentication, for example-to assure secure...

23/3,K/6 (Item 6 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2005 ProQuest Info&Learning. All rts. reserv.

01788746 04-39737

Protecting your web site against credit-card fraud

Morgan, Cynthia

Computerworld v33n10 PP: 71 Mar 8, 1999

ISSN: 0010-4841 JRNL CODE: COW

WORD COUNT: 921

...DESCRIPTORS: **Electronic commerce** ;

...ABSTRACT: anomalies in a cardholder's buying routines. The best defense institutes screening practices based on **online retailers** ' most typical sales. A high percentage of fraud originates from free e-mail addresses. Banks...

TEXT: Headnote:

AI tools can reduce risks; but fresh phony cards are a click away

ELECTRONIC - COMMERCE merchants focus on making customers feel safe inside their virtual stores (see story, page 24...

...can be had for as little as \$25 online, said Ramzi Saffouri, a consultant at **fraud - detection** software maker Advanced Software Applications Corp. in Pittsburgh.

According to the Federal Bureau of Investigation...

...to be [America Online Inc.] officials and ask for billing confirmation," said Bill Burnham, an **electronic - commerce** analyst at Credit Suisse First Boston Bank in San Francisco. "There's always a newcomer...

...Inc. in Olney, Md., whose Internet ScamBusters site (www.scambusters.org) serves around 50,000 **electronic - commerce** merchants.

Banks and credit-card processors use artificial intelligence systems to discover anomalies in a...

...costly.

Even then, "We've learned that you have to have a human behind every **Internet transaction** , monitoring the process," Shanks said.

"The more it costs, the more someone will try to...

...to sell the really expensive products online."

The best defense institutes screening practices based on **online retailers** ' most typical sales. Administrators flag addresses that don't match and other suspicious details. "We...

...agrees to perform additional checks. "If we ship to the same bill-to/ship-to **address** , we call them to **verify** and we document that - some banks won't charge us. And our developers agree to...

...said. "That way, we both lose the profit we would have made, but no more."

Electronic - commerce security managers shouldn't rely too heavily on expiration-date checks, said one industry insider...

23/3,K/7 (Item 7 from file: 15)

DIALOG(R)File 15:ABI/Inform(R)

(c) 2005 ProQuest Info&Learning. All rts. reserv.

01771209 04-22200

The law and CPA WebTrust

Pacini, Carl; Sinason, David

Journal of Accountancy v187n2 PP: 20-24 Feb 1999

ISSN: 0021-8448 JRNL CODE: JAC

WORD COUNT: 2786

...TEXT: this new assurance service? The law ultimately will evolve with regard to assurances linked to **electronic commerce**, but for now the well-prepared CPA will want to know precedents and strategies that...

...responsibilities. Various groups have concluded that the public assigns independent accountants a greater responsibility for **detecting** and reporting **fraud** and financial misinformation than can be met. Many e-commerce consumers may not understand the...

...business electronically," according to the AICPA/CICA WebTrust Principles and Criteria for Business-to-Consumer **Electronic Commerce**. (Go to www.aicpa.org/webtrust/index.htm.)

Financial statement users who suffer investment or...Table Omitted)
Captioned as: U.S. Case Law With Parallels to WebTrust

3. Quantify risk- **estimate potential** monetary damages.

4. Evaluate the risks and rewards of offering a service.

A CPA is...

...to determine whether they conform to the WebTrust Principles and Criteria for Business-to-Consumer **Electronic Commerce** and (2) has issued an assurance services report with an unqualified opinion. Cautionary language should...

23/3,K/8 (Item 8 from file: 15)

DIALOG(R)File 15:ABI/Inform(R)

(c) 2005 ProQuest Info&Learning. All rts. reserv.

01749067 04-00058

Information highway robbery

Oberndorf, Shannon

Catalog Age v15n13 PP: 59 Dec 1998

ISSN: 0740-3119 JRNL CODE: CTA

WORD COUNT: 511

...DESCRIPTORS: **Electronic commerce** ;

...ABSTRACT: according to credit card processor Paymentech. And the losses may skyrocket with the growth of **electronic commerce**. Your best bet

for controlling online credit fraud may be setting up your own program...
...TEXT: according to credit card processor Paymentech. And the losses may skyrocket with the growth of **electronic commerce** .

For one thing, "print catalogers can exclude suspect consumers from the mailing," says John Shirey, senior director of **electronic commerce** at Paymentech. "But online, controlling who visits your site isn't possible. Anyone can visit...

...secrets in online chat rooms. Many hackers can get around traditional stopgaps such as the **Address Verification System (AVS)**, a service from credit card issuers and processors that passes the cardholder's...

...000 a month in fraudulent bids from stolen credit cards, until it developed a proprietary **fraud detection** system, says cofounder/chief technical officer Alan Fisher.

The Menlo Park, CA-based marketer's...

...number appears in the database, Onsale automatically stops the bid.

(Illustration Omitted)

Captioned as: A **fraud detection** system has helped auction site Onsale cut monthly fraud losses in half.

Successful bids then...

...SO

TIPS TO TACKLE WEB FRAUD

Use all available credit card screening systems, such as **Address Verification System (AVS)** and CID verification.

Establish your own fraud prevention controls. For instance, computer marketer...

...certain amount before shipping the goods. But don't rely solely on e-mail to **verify** orders or "ship to" **addresses** , because a hacker using a stolen credit card number will likely use his own e-mail **address** for **verification** .-SO

23/3,K/9 (Item 9 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2005 ProQuest Info&Learning. All rts. reserv.

01686889 03-37879

A security blanket for the Internet

Lucas, Peter

Credit Card Management v11n5 PP: 33-37 Aug 1998

ISSN: 0896-9329 JRNLCODE: CCM

WORD COUNT: 2348

DESCRIPTORS: **Electronic commerce** ;

ABSTRACT: As **electronic commerce** begins to grow, so does fraud on the Internet. And that means the card industry...

TEXT: Headnote:

As **electronic commerce** begins to grow, so does fraud on the Internet. And that means the card industry...

...as 60% of volume. To make matters worse, fraud losses are predicted to escalate as **electronic commerce** rockets. New Le

That's because the newness of the medium and the inexplicable trust...

...operations officer for the National Fraud Center, a Horsham, Pa.-based consulting firm specializing in **fraud prevention and detection**. "The Internet is a new medium to reach millions of people and gives a scam...

...Visa U.S.A. last December formed SETCo., a company chartered to establish the Secure **Electronic Transaction** standard (SET) for the Internet.

SET, which as of April was being piloted in 34...

...is such fertile ground for credit card fraud. First, there is the push to grow **electronic commerce** and make credit and debit cards the currency of the Internet. Second, consumers willingly surrender...

...respective computers that verify that the account data being exchanged during the course of an **Internet transaction** are legitimate.

"SET is authentication tied to the transaction," says Stephen Herz, senior vice president of **electronic commerce** for Visa International.

"Merchants want to be sure the cardholder has a valid relationship with... of SET software will be certified by SETCo.," says Andrew H. Bartels, vice president of **electronic commerce** for AmEx. "Vendors must put their product through a testing process to demonstrate that it..."

...they are imitating. "Spoofing is a real problem on the Internet because Web site URLs (**addresses**) have no **authentication** ," says American Express's Bartels.

SET combats sniffers and spoofing by encrypting financial data. Even...

...browsers and merchant Web sites already support the technology, says Colleen Zambole, vice president of **electronic commerce** , Discover Card. "The sites that support SSL have not had data on card transactions compromised..."

...SET becomes an industry standard, he remains confident SET will become the encryption standard for **electronic commerce** . "There are a lot of pieces that have yet to fall in place to move..."

...one piece of the Internet security puzzle. Internet-related card fraud is not limited to **electronic commerce** . Identity theft is a major problem. Indeed, there are a number of scams that allow...system without ever physically penetrating its four walls," he said.

Beating the System

Further, as **electronic commerce** grows, the era of computer hackers being motivated solely by the thrill of beating the...

...will have to aggressively act to suppress fraud and other criminal activity. "The challenge of **electronic commerce** is the security of the data provided and received," says Kerins. "If that confidence is not there, then the success of **electronic commerce** is questionable."

23/3,K/10 (Item 10 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2005 ProQuest Info&Learning. All rts. reserv.

01605867 02-56856

Mining your own business

Foley, John; Russell, Joy D
Informationweek n673 PP: 18-20 Mar 16, 1998
ISSN: 8750-6874 JRNL CODE: IWK
WORD COUNT: 1649

...ABSTRACT: standing barriers to deployment. Increasingly, these products are being tuned for specific applications - such as **fraud detection** or customer-relationship management - and for vertical industries. Oracle Corp. will soon unveil a marketing...

...release of its database, Oracle8.1. Microsoft Corp. is incorporating data mining technology into its **electronic - commerce** system, Site Server 3.0 Commerce edition. ...

...TEXT: that range from identifying which hotel guests might want a cigar in their rooms to **detecting** stock market **fraud**.

Data mining, which uses mathematical algorithms to find patterns in data, is in the midst...

...long-standing barriers to deployment. Increasingly, these products are being tuned for specific applications such as **fraud detection** or customer relationship management and for vertical industries.

Also, two leading software vendors Oracle and Microsoft are...

...Discovery, SPSS, SRA International, and Thinking Machines.

Microsoft is incorporating data mining technology into its **electronic - commerce** system. Microsoft's Site Server 3.0 Commerce edition, due next quarter, will come with...

...senior technical specialist with NASD Regulation. Still, data mining has been invaluable in helping to **detect fraud**, Cooper says, adding: "The answer is in the data."
Too Difficult?

Nearly two-thirds of...

...Mateo, Calif., will unveil a data mining software bundle designed to automate marketing efforts by **comparing** proposed campaigns against existing **customer data**.

Scott Toborg, a data mining specialist with SBC Technology Resources, the advanced technologies unit of...

23/3,K/11 (Item 11 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2005 ProQuest Info&Learning. All rts. reserv.

01545978 01-96966

Assurance service opportunities: Implications for academia

Elliott, Robert K
Accounting Horizons v11n4 PP: 61-74 Dec 1997
ISSN: 0888-7993 JRNL CODE: ACH
WORD COUNT: 6069

...TEXT: expectations of auditors, together with pressures for greater accountability, will increase demands for auditors to **detect fraud** and illegal acts, and provide early warning of financial distress and going concern problems.

How...

...needs.

The table has research implications. The academic community can help to improve techniques to **detect fraud** and illegal acts. It can help improve techniques to evaluate financial distress and going-concern... criteria. (www.aicpa.org/assurance/scas/newsvs/reliab/index.htm) Assess whether informational features of **electronic commerce** function in accordance with accepted criteria. The service would provide assurance with respect to the integrity, security and privacy of **electronic transactions**, electronic documents and the supporting systems. (www.aicpa.org/assurance/scas/newsvs/elec/index.htm...

...background in attestation would therefore be fundamental to preparing to perform them.

Systems assurance and **electronic - commerce** assurance show again the usefulness of improving the treatment of information technology in the curriculum. Assurers providing **electronic - commerce** assurance services need to understand the risks of **electronic commerce** (e.g., intentional attacks, transmission failures, lack of authentication, lack of trust, theft of identity...

...long after this writing.

Assurance services will be necessary to maximize the growth of the **electronic - commerce** marketplace, and non-CPAs are capable of gearing up to provide the services. Consumers will not participate in **electronic commerce** unless they have confidence that they have reached a properly identified website, that their personal...

...can be stolen and used to drain their assets. Even CPAs who do not provide **electronic - commerce** assurance services must understand **electronic - commerce** information systems and information flows, because in time they will be entwined with all sorts...criteria:

Information systems reliability-Criteria for assessing the reliability of all major internal information systems.

Electronic commerce -Criteria for assessing the integrity and security of **electronic commerce**.

Health care performance measurementCriteria for assessing the quality of service provided by care givers.

In...technology experience in light of the competency needed to evaluate the security and integrity of **electronic - commerce** information? How helpful is their training in performance measurement in light of the demands on...and the waste of capital, talent, technology and materials.

Secure information will be essential to **electronic commerce**, and high-quality information will be essential to sound decisions on economic, social and political...

...not, and would not be, the sole or major suppliers of accounting firm consultants.

Consider **figure 5**, which illustrates the **likely** effects of a failure to expand new assurance services.² It shows a declining proportion...

...in 1990.

The growth in personnel from growth in assurance services has a basis in **estimates** of the revenue **potential** of new assurance services. The estimates were prepared by the Special Committee on Assurance Services...

23/3,K/12 (Item 12 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2005 ProQuest Info&Learning. All rts. reserv.

01506732 01-57720
Fraud detection and more
Ring, Trudy
Credit Card Management v10n6 PP: 128-129 Sep 1997
ISSN: 0896-9329 JRNL CODE: CCM
WORD COUNT: 900

Fraud detection and more

ABSTRACT: Providers of **fraud - detection** software are the card industry's ultimate specialists, but even they are expanding their product...

...activity, has in the past few years become popular for use in programs designed to **detect** credit card **fraud** by spotting transactions inconsistent with the cardholder's usual pattern. HNC Software Inc, whose Falcon **fraud - detection** software is used by 40 of the top 50 credit card issuers, recently introduced software...

...TEXT: specialists are branching out as they find new uses for their core technology.

Providers of **fraud - detection** software are the card industry's ultimate specialists, but even they are expanding their product...

...activity, has in the past few years become popular for use in programs designed to **detect** credit card **fraud** by spotting transactions inconsistent with the cardholder's usual pattern. The dominant providers of neural...

...and Nestor Inc., Providence, R.I. Today, though, they are expanding their product lines beyond **fraud detection** and putting themselves into competition with some other software specialists.

HNC, whose Falcon **fraud - detection** software is used by 40 of the top 50 largest credit card issuers, recently began...

...cardholder profitability.

Nestor, meanwhile, has expanded upon its Prism CardAlert product, which is designed to **detect fraudulent** credit card use, by developing systems

targeting application fraud, debit card fraud, and merchant fraud, and, in a move away from the fraud arena, software to **gauge** the **likelihood** that a cardholder will go bankrupt.

Logical Moves?

But HNC and Nestor officials say these...

...Nestor recently signed an agreement with Omahabased Applied Communications Inc., a provider of software for **electronic commerce**, by which ACI will make all of Nestor's **fraud - detection** products available to ACI's 500-plus clients in more than 67 countries. Waterloo, Belgium...

...bank card association Europay International, a MasterCard International partner, is using Nestor's Prism MerchantAlert **fraud - detection** system for Artemis, a new Europay service aimed at catching fraud by monitoring merchant behavior...

23/3,K/13 (Item 13 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2005 ProQuest Info&Learning. All rts. reserv.

01444922 00-95909

The growth of network computing

Wyckoff, Andrew

OECD Observer n206 PP: 41-44 Jun/Jul 1997

ISSN: 0029-7054 JRNL CODE: OED

WORD COUNT: 2556

...ABSTRACT: network computing will be on the broader economy as it provides the enabling infrastructure for **electronic commerce**.

...TEXT: the existing computing infrastructure is interconnected.1

The development of the Internet has made it **possible** to connect **computers** of different designs and operating systems at a relatively low price, largely using the existing...

...presence of a computer in the home: for every \$10,000 increase in income, the **likelihood** of owning a **computer** increases by 7 percentage points. PC ownership is also directly correlated with type of education... and the more people it attracts.

of the Cyber-economy? Three recent innovations in network **computing** now make the **potential** of **electronic commerce** a reality: the widespread diffusion of the Internet and its associated applications like the WorldWide...

...be used for 'high-end' applications that require guaranteed, reliable service. One of these is **electronic commerce**. Few people will want to locate a business where customers cannot reach them. The causes...

...Captioned as: Figure 2

(Graph Omitted)

Captioned as: Figure 1

Mining

To exploit the economic **potential** of network **computing** fully both for the seller and the buyer, techniques must be developed that accommodate the ...

...on data bases in excess of a gigabyte such as the hundreds of gigabytes of **electronic point-of-sale** data collected by supermarkets. Data-mining technologies have the potential to transform markets and businesses...

...market on a one-to-one basis that many see as a distinguishing factor of **electronic commerce**. The ability to do so raises some potentially serious privacy issues of a new sort...has many positive aspects as well. It is very effective, for instance, in helping to **detect fraud**, especially in **electronic commerce transactions** that may be of small value but in huge volumes. It is already being used...

...biggest impact will be on the broader economy as it provides the enabling infrastructure for **electronic commerce**.

(Photograph Omitted)

Captioned as: Its own worst enemy? As people find the Internet easier to...

23/3,K/14 (Item 14 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2005 ProQuest Info&Learning. All rts. reserv.

01419942 00-70929

AOL doesn't suck!

Monash, Curt; Barlow, Linda
Upside v9n5 PP: 76-88+ May 1997
ISSN: 1052-0341 JRNL CODE: UPS
WORD COUNT: 6590

...TEXT: such as health, entertainment or personal finance, then AOL can easily direct focused advertising and **electronic commerce** at them.

In some cases, this approach might work. Interactive games, for example, have a AOL's customers fall into well-educated, upscale demographic groups, who are **likely** to use **computers** at work or in school. Consequently, they are likely to become increasingly familiar with standard...

...opportunity (other than chat and games): providing information and selling goods. Hit-or-miss, mall-like **on-line shopping** may be interesting to some consumers, but most people will prefer more efficient on-line...

...indefinitely. If it doesn't clean up its software act in time, AOL's whole **electronic-commerce** business model could crash, taking the information-oriented channels down with it.

Thus, the all-encompassing...problems solve each other and claim, a la the American Express Card, to provide enhanced **fraud** protection by **detecting** major deviations from your "usual" system usage.

Another way AOL can make money from direct **on-line sales** of products and services is "affinity marketing" of specialized products associated with various content areas...

...of eyeballs.

But books and peripherals may prove to be chump change compared with another **electronic - commerce** opportunity. Many technology vendors have fruitlessly fantasized about imposing a "toll" on an unending series... middleman.

(Table Omitted)

Captioned as: AOL's Words That Suck

The big kahuna of all **on - line commerce** ventures to date is AOL's deal with Tel-Save Holdings Inc. of New Hope...

...already collected a \$100 million prepayment, plus warrants on Tel-Save stock.

Overall, AOL's **on - line commerce** story seems compelling: a world of computerliterate cocooners, merrily disintermediating from the comfort of their...

23/3,K/15 (Item 15 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2005 ProQuest Info&Learning. All rts.. reserv.

01144346 97-93740
Good news on fraud
Kiley, Kathleen
Catalog Age v12n9 PP: 5, 33 Sep 1, 1995
ISSN: 0740-3119 JRNL CODE: CTA
WORD COUNT: 913

...TEXT: June, for example, MasterCard launched its Address Information Management Service system (AIMS) to help marketers **check** billing **addresses** against "ship to" addresses.

Using the system, catalogers have online access to MasterCard's global network Banknet, which enables them to immediately **verify** that a "shipped to" **address** is the same as the customer's billing address. A discrepancy can tip-off the...

...revenue. In addition to MasterCard's AIMS, The Right Start relies on Visa International's **Address Verification** Service (AVS). The mailer has also trained its telemarketers to watch for orders over \$150...

...Little & Co. Unfortunately, she says, the increased use of express delivery by catalogers has made **fraud detection** harder.

To combat credit card fraud, Christie encourages all catalogers to keep a file on...

...card fraud will always be a problem for direct marketers. And as catalogers move toward **electronic commerce**, the problem will intensify as personal contact decreases further. The card issuers are already working to develop more sophisticated devices to **detect fraud**. But until such prevention devices exist, "it's an exposed arena for the perpetrators," Murayama...

...REQUEST CREDIT CARD I.D. NUMBERS

5. MAINTAIN A FILE OF PREVIOUS OFFENDERS
6. USE **ADDRESS VERIFICATION SERVICES**
7. BALANCE REFUND ACCOUNTS AGAINST SALES ACTIVITY

SOURCE: LITTLE & CO.

23/3,K/16 (Item 16 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2005 ProQuest Info&Learning. All rts. reserv.

01122821 97-72215

To catch a thief

van de Vliet, Anita

Management Today PP: 70-74 Oct 1995

ISSN: 0025-1925 JRNL CODE: MTO

WORD COUNT: 2473

...TEXT: firm,' comments Farrall. 'It's also really pitiful,' he says, because this steady programme of **theft** could have been **detected** long before. It was in many ways a classic case. The 'faithful old retainer', in ...

...Crime--Managing the Business Risk, although statistically out of date, gives some idea of the **possible** overall scale. This **estimated** that crime against business costs well over L5 billion a year, and remarked that some...also numerous practical measures that companies can and do use to stop theft. Advances in **Electronic Point of Sale** (EPOS) technology, for example, are making it more difficult for potential shoplifters to saunter out...Lorraine Electronics Surveillance, sophisticated bugging devices are now being used by 'most quoted companies' to **detect theft** and conspiracy at work. Smaller companies unable to afford such wizardry can still apply the...

23/3,K/17 (Item 1 from file: 610)
DIALOG(R)File 610:Business Wire
(c) 2005 Business Wire. All rts. reserv.

00158025 19991215349B1665 (USE FORMAT 7 FOR FULLTEXT)
INTELLI-CHECK Announces Underwriters Exercise of Over-allotment Option; Company Names Two New Board Members
Business Wire
Wednesday, December 15, 1999 15:51 EST
JOURNAL CODE: BW LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 528

...company. Mr. Levy has a specialized interest in the prevention of drunk driving, a problem **addressed** by Intelli- **Check** 's proprietary software. Howard Davis has hands-on operating experience as Chief Executive Officer of...

...identification, passports, and other forms of government-issued identification. Additionally, ID Check is capable of **detecting fraudulent** or altered documents

Copyright (C) 1999 Business Wire. All rights reserved.

Distributed via COMTEX.

-0-

CONTACT: Frank Mandelbaum
Chairman
516/421-2011

GEOGRAPHY: NEW YORK

INDUSTRY CODE: TELECOMMUNICATIONS
NETWORKING
HARDWARE
INTERNET
RETAIL
RESTAURANTS
PRODUCT
MANAGEMENT
CHANGES

23/3,K/18 (Item 2 from file: 610)
DIALOG(R)File 610:Business Wire
(c) 2005 Business Wire. All rts. reserv.

00146756 19991129333B1147 (USE FORMAT 7 FOR FULLTEXT)
HotOffTheWire.com Leverages CyberSource Internet Fraud Screen and Credit Card Payment Services; Retailers and Manufacturers Benefit With Secure Online Purchasing
Business Wire
Monday, November 29, 1999 08:48 EDT
JOURNAL CODE: BW LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 540

... CyberSource Internet Fraud Screen and Credit Card Payment Services; Retailers and Manufacturers Benefit With Secure Online Purchasing

TEXT:

...com Web
site. Now for the first time, manufacturers using HotOffTheWire.com can process secure **Internet** credit card **transactions** in real time.

"By working with CyberSource to offer a range of Payment Services from the CyberSource **Internet Commerce Suite(SM)**, our suppliers can grow their businesses with the confidence that their back-end...
...through HotOffTheWire.com, our suppliers have access to real time credit card authorization, credit card **fraud detection** and delivery **address verification**. By outsourcing these services, our suppliers can concentrate on building their businesses."

...HotOffTheWire.com, CyberSource launches three applications to process the transaction in real-time: credit card **authentication**, **fraud detection** and delivery **address verification**

"To transition their purchasing decisions to the **Internet**, **retailers** and manufacturers need to see a significant business benefit and be assured of the high...

...developer and provider of eCommerce

transaction services, and a pioneer in the area of Internet **fraud detection**. More than 800 Internet merchants in more than 26 countries have chosen to use CyberSource services. CyberSource provides mission-critical reliability with the CyberSource **Internet Commerce Suite**(SM), offering merchant-controlled, real-time services including Payment Services, Tax Services, Risk Management...
...the Web at <http://www.HotOffTheWire.com>.

CyberSource is a U.S. registered trademark. CyberSource **Internet Commerce Suite** is a service mark of CyberSource Corporation. All other brands and product names are...

...Lisa Beyer, (781) 684-0770
markm@schwartz-pr.com

GEOGRAPHY: MASSACHUSETTS

INDUSTRY CODE: COMPUTERS/ELECTRONICS
INTERNET
E- **COMMERCE**
RETAIL

23/3,K/19 (Item 3 from file: 610)
DIALOG(R)File 610:Business Wire
(c) 2005 Business Wire. All rts. reserv.

00122570 19991019292B0191 (USE FORMAT 7 FOR FULLTEXT)
RISKWISE.COM Introduces New Weapon to Combat Credit Card Fraud On the Internet
Business Wire
Tuesday, October 19, 1999 08:48 EDT

JOURNAL CODE: BW LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 499

...well known e-commerce services.

"This product helps merchants find additional profitable sales opportunities in **address verification** failures and has been proven to identify seventy-five percent of chargebacks in the ten...

...1999, riskwise.com is a wholly owned subsidiary of RiskWise International providing risk management and **fraud detection** services designed to safeguard **Internet transactions**. Its primary products, SureSale and Chargeback Defender, are designed to help e-merchants identify more...

23/3,K/20 (Item 4 from file: 610)
DIALOG(R)File 610:Business Wire
(c) 2005 Business Wire. All rts. reserv.

00103304 19990914257B1352 (USE FORMAT 7 FOR FULLTEXT)
US Dataworks, Thomson Financial Publishing and CheckFree Announce Alliance to Enhance Returnworks, a Re-Presented Check Entry -RCK- Processing Module
Business Wire
Tuesday, September 14, 1999 10:18 EDT
JOURNAL CODE: BW LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT

DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 735

TEXT:

...administrative, non-fund related errors have been one of the biggest barriers associated with converting **check** MICR to ACH. EPICWare **addresses** these errors before they occur." US Dataworks embedded Thomson's EPICWare Filter source code within...

...cash flows, lowering costs due to less human involvement, and creating an opportunity for earlier **fraud detection**.

"The demand for financial institutions to process Re-presented Check Entries (RCKs) will increase dramatically...

...com) develops and distributes highly specialized information and applications for the banking, financial services, and **electronic commerce** sectors. TFP's 200,000 clients around the world use the information to expedite payments processing and ensure compliance, streamline research and analysis, enhance **electronic commerce**, and market their products and services. Thomson Financial Publishing is a division of Thomson Financial...

...checkfree.com), the operating subsidiary of CheckFree Holdings Corporation, is the leading provider of financial **electronic commerce** services, software and related products. CheckFree designs, develops and markets services that enable nearly three...

...to make electronic payments and collections, automate paper-based recurring financial transactions and conduct secure **Internet transactions**.

Copyright (C) 1999 Business Wire. All rights reserved.

-0-

CONTACT: Thomson Financial Publishing
Bob McKay...

...INDUSTRY NAMES: **ELECTRONIC COMMERCE** ;

23/3,K/21 (Item 5 from file: 610)
DIALOG(R)File 610:Business Wire
(c) 2005 Business Wire. All rts. reserv.

00067056 19990628179B1484 (USE FORMAT 7 FOR FULLTEXT)
Internet Merchants Face Rising Credit Card Fraud and Chargeback Fees; Good Customer Service Keeps Chargeback Fees Down
Business Wire
Monday, June 28, 1999 13:42 EDT
JOURNAL CODE: BW LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 328

TEXT:

...the Internet," states that credit cards dominate as the electronic payment method of choice for **online shoppers**, even though the use of E-checks and debit cards offers better user verification.

...will threaten

the viability of their E-business," observes GartnerGroup analyst Ken Kerr. "While a **fraud detection** system is essential for accurate credit card verification, a high number of chargebacks on **Internet purchases** are the result of customer disputes, not fraud."

To limit customer disputes, merchants should: - Provide...
...including taxes and shipping costs; - Provide customer service contact information.

The report also identifies several **fraud detection** methods, including **address verification** services, rules-based screening services, card verification methods and digital certificate systems.

About GartnerGroup

As...

...INDUSTRY NAMES: **ELECTRONIC COMMERCE** ;

23/3,K/22 (Item 6 from file: 610)
DIALOG(R)File 610:Business Wire
(c) 2005 Business Wire. All rts. reserv.

00039741 19990504124B0198 (USE FORMAT 7 FOR FULLTEXT)
ProCart Provides Smart, Secure Online Transaction Processing That Equals Money in the Bank for e-stores
Business Wire
Tuesday, May 4, 1999 11:29 EDT
JOURNAL CODE: BW LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 1,406

ProCart Provides Smart, Secure Online Transaction Processing That Equals Money in the Bank for e-stores

...to
manage and track sales, payments, shipments, inventories, taxes, returns, credits, and much more.

"With **online shopping** revenues expected to exceed \$12 billion in 1999(a), successful e-stores need more than...

...that
enhances a customer's perception of the company and facilitates a secure environment for **online purchases**. ProCart was developed specifically to enable e-stores to make the shopping experience simple and...

...and much
more.

ProCart Deluxe extends order management to shoppers, enabling them to check status **online**. **Shoppers** can check status on orders, shipments, returns, credits, and more. Rigney said, "Empowering shoppers to...

...orders and shipments helps create a comfortable shopping environment."

Both merchants and shoppers can easily **check UPS shipping** records

through online connections provided by ProCart. Specific delivery information is available for multiple shipments...time \$2,495 set-up fee. Includes extended merchant interface, extended tax module, CardSentry(TM) **Fraud Detection** Module, MultiShip(TM) Module, OrderTrak(TM) Module, Extended Tax Module, and Merchant Warehouse Manager.
For...

...INDUSTRY NAMES: **ELECTRONIC COMMERCE ;**

23/3,K/23 (Item 1 from file: 810)
DIALOG(R)File 810:Business Wire
(c) 1999 Business Wire . All rts. reserv.

0889894 BW0072

HNC SOFTWARE: HNC Software Unveils Check Fraud Detection Solution; Falcon Cheque to Attack \$1 Billion Problem

August 05, 1998

Byline: Business Editors

HNC Software Unveils Check Fraud Detection Solution; Falcon Cheque to Attack \$1 Billion Problem

...States, HNC Software Inc. today announced the general availability of Falcon Cheque(TM), a check **fraud detection** solution that builds upon HNC's proven predictive software technologies currently used by top bank...

...president of HNC's Financial Solutions division. "Given the proven effectiveness of HNC's intelligent **fraud detection** technology, we almost felt as though we had a moral imperative to develop a product to **address checking** account fraud."

Currently monitoring over 240 million credit card accounts at banks worldwide, HNC's Falcon(TM) credit card **fraud detection** solution is generally credited with helping to curtail the meteoric rise in credit card fraud...

...project with a major US bank, HNC has demonstrated that Falcon Cheque provides strong, quantifiable **fraud detection**. Because of the intuitive and automated data mining provided by the neural network technology, Falcon...

...environments. HNC provides innovative predictive software systems in the financial services, retail, insurance information, and **electronic commerce** markets. For more information, see www.hnc.com or contact Patsy Campbell, Director of Marketing...

Set	Items	Description
S1	124234	FRAUD? OR DECEPTION? OR THEFT OR THIEV? OR LARCENY OR STEA- L? OR ROBBERY OR CHEAT? OR SWINDL? OR DISHONEST?
S2	1644650	CALCULAT? OR DETERMIN? OR COMPUT??? OR FIGURE??? OR ESTIMA- T? OR GAUG?
S3	1064933	POTENTIAL? OR LIKELIHOOD OR RELATIVE OR POSSIBL? OR PROBAB- LE OR PROBABILITY OR LIKELY
S4	939415	CHECK??? OR COMPAR??? OR VERIFY? OR VERIFI? OR CONFIRM??? - OR VALIDAT? OR AFFIRM? OR CORROBORAT? OR AUTHENTICAT?
S5	541196	(PURCHASER? OR BUYER? OR SHOPPER? OR CONSUMER? OR CUSTOMER? OR USER?) (1W) (DATA OR INFO OR INFORMATION) OR SHIP()TO OR SH- IPPING OR BILL()TO OR ADDRESS? OR AREA()CODE? OR PHONE()NUMBE- R? OR ZIP
S6	905236	RISK OR RISKS OR CHANCE OR SCORE
S7	28355	S2(4N)S3
S8	4049	S4(4N)S5
S9	907	S7 AND S1
S10	13	S9 AND S8
S11	6	S10 NOT PY>1999
S12	5	RD (unique items)
S13	1108136	NON()PERSONAL OR NONPERSONAL OR ELECTRONIC OR ON()LINE OR - ONLINE OR INTERNET OR DIGITAL?
S14	2349777	TRANSACTION? OR SALE? OR COMMERCE OR SHOP? OR RETAIL? OR - SELLING OR PURCHAS? OR MARKETING
S15	121250	S13(2W)S14
S16	5386	S15 AND S1
S17	224	S16 AND S8
S18	65	S17 NOT PY>1999
S19	37	S18 AND (S7 OR S6)
S20	33	RD (unique items)

File 613:PR Newswire 1999-2005/Oct 27

(c) 2005 PR Newswire Association Inc

File 813:PR Newswire 1987-1999/Apr 30

(c) 1999 PR Newswire Association Inc

File 634:San Jose Mercury Jun 1985-2005/Oct 26

(c) 2005 San Jose Mercury News

File 624:McGraw-Hill Publications 1985-2005/Oct 27

(c) 2005 McGraw-Hill Co. Inc

20/3,K/1 (Item 1 from file: 613)

DIALOG(R)File 613:PR Newswire

(c) 2005 PR Newswire Association Inc. All rts. reserv.

00232608 19991215SFW034 (USE FORMAT 7 FOR FULLTEXT)

CyberSource(R) Powers bankone.com

PR Newswire

Wednesday, December 15, 1999 08:01 EST

JOURNAL CODE: PR LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT

DOCUMENT TYPE: NEWSWIRE

WORD COUNT: 503

TEXT:

...of real-time eCommerce transaction services, today announced that it now provides payment processing and **risk** management services for Bank One Corporation's (NYSE: ONE) financial supersite, bankone.com.

Bankone.com...

...they turned to CyberSource for a secure and scalable solution for conducting and managing these **online transactions**.

"Our site is designed to provide Bank One customers with the most comprehensive set of...

...customer service and reliability. After an extensive evaluation, we selected CyberSource for its scalability, superior **fraud** screening service, very high level of data security and their expertise in providing and managing...

...it is imperative that eCommerce leaders such as bankone.com implement services that minimize their **risk** of **fraud** and are proven to be secure and reliable," said Steve Klebe, vice president of payment...

...back-end eCommerce transaction services and avoid major investments in software and staffing. The CyberSource **Internet Commerce** Suite of services includes: Credit Card Services, Tax Calculation, Internet **Fraud** Screen enhanced by Visa, Fulfillment Messaging, Delivery **Address Verification**, Digital Delivery, Digital Warehousing, Policy Compliance, and Export Compliance.

About CyberSource

CyberSource is a leading developer and provider of eCommerce transaction services, and a pioneer in the area of Internet **fraud** detection. More than 800 Internet merchants in more than 26 countries have chosen to use CyberSource services. CyberSource provides mission-critical reliability with the CyberSource **Internet Commerce** Suite(SM), offering merchant-managed, real-time services including, Payment Services, Tax Services, **Risk**

Management
Services, Distribution Control Services, and Fulfillment Management
Services.
Customers of CyberSource include leading Internet...
...cybersource.com or
ir@cybersource.com

NOTE: CyberSource is a U.S. registered trademark. CyberSource
Internet
Commerce Suite is a service mark of CyberSource Corporation. All other
brands
and product names are...

...COMPANY NAMES: **RISK** MANAGEMENT

20/3,K/2 (Item 2 from file: 613)
DIALOG(R)File 613:PR Newswire
(c) 2005 PR Newswire Association Inc. All rts. reserv.

00228197 19991208DAW010 (USE FORMAT 7 FOR FULLTEXT)
**TeleCheck Reaches Billion Dollar Mark With Electronic Check Acceptance
Service**
PR Newswire
Wednesday, December 8, 1999 07:01 EST
JOURNAL CODE: PR LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 673

TEXT:
...First Data
Corp. (NYSE: FDC), today announced that it has settled one billion dollars
of
electronic transactions since the nationwide introduction of the
TeleCheck(R)
Electronic Check Acceptance(SM) (ECA(R)) service...

The consumer then simply signs a printed receipt authorizing the
electronic transaction and the cancelled paper check, along with a copy
of the
authorization slip, is returned...

...statement for
reconciliation purposes, and consumers retain the same rights as today in
disputing any **fraudulent** items posted to their account. In addition,
since
the check writer keeps the cancelled physical **check**, the **risk** of name,
address
and other personal information being used **fraudulently** is substantially
reduced.

"Having processed over a billion dollars of **electronic transactions**
in 18
months indicates that ECA(R) is reaching critical points in market
acceptance," said...

...210,000 retail, financial institution, grocery and
other industry clients to increase their profitability, reduce **risk** and
streamline operations. TeleCheck's check acceptance and **electronic**

commerce

solutions help businesses safely and efficiently accept payment at the point of sale, by telephone...

...Atlanta-based First Data Corp. helps move the world's money. As the leader in **electronic commerce** and payment services, First Data serves more than two million merchant locations, 1,400 card...

...INDUSTRY NAMES: **ELECTRONIC COMMERCE** ;

20/3,K/3 (Item 3 from file: 613)
DIALOG(R)File 613:PR Newswire
(c) 2005 PR Newswire Association Inc. All rts. reserv.

00223832 19991201SFW016 (USE FORMAT 7 FOR FULLTEXT)
CyberSource(R) Powers City Halls Across the U.S. as They Serve Residents And Businesses Online
PR Newswire
Wednesday, December 1, 1999 08:01 EST
JOURNAL CODE: PR LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 677

TEXT:

...eCommerce transaction services, today announced that City Halls across the USA are deploying the CyberSource **Internet Commerce** Suite to power real-time credit card transactions for their online community services.

(Photo: <http...>

...site grows, the city plans to "switch on" additional CyberSource services, such as the Internet **Fraud** Screen enhanced by Visa, designed to reduce online **fraud** to less than one percent, and **address verification**, designed to prevent incorrectly entered delivery addresses costing the city with needless merchandise returns. The...

...developer and provider of eCommerce transaction services, and a pioneer in the area of Internet **fraud** detection. More than 800 Internet merchants in more than 26 countries have chosen to use CyberSource services. CyberSource provides mission-critical reliability with the CyberSource **Internet Commerce** Suite(SM), offering merchant-controlled, real-time services including, Payment Services, Tax Services, **Risk** Management Services, Distribution Control Services, and Fulfillment Management Services. Customers of CyberSource include leading Internet...
...com
or ir@cybersource.com.

NOTE: CyberSource is a U.S. registered trademark. The "CyberSource

Internet Commerce Suite" is a service mark of CyberSource Corporation.
All
other brands and product names are...

...COMPANY NAMES: **RISK MANAGEMENT**

20/3,K/4 (Item 4 from file: 613)
DIALOG(R)File 613:PR Newswire
(c) 2005 PR Newswire Association Inc. All rts. reserv.

00216154 19991116LATU022 (USE FORMAT 7 FOR FULLTEXT)
**Micro General Ranked #1 Fastest-Growing Company in Orange County This Year
By Orange County Business Journal**
PR Newswire
Tuesday, November 16, 1999 06:00 EST
JOURNAL CODE: PR LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 904

...Escrow.com(TM), Inc., - comprehensive e-commerce solution that protects
both buyers and sellers against **fraud**. The company plans to launch the
site
in late 1999. Escrow.com is a stand...

...sites. Escrow.com's products and services include:

- Escrow services for auctions, classified and other **Internet**
-enabled
transactions ;
- Master-merchant transaction services for all forms of portal and
Internet commerce ;
- **Shipping** , **authentication** , appraisal and financing services.

L.D. Exchange, Inc. - is a facilities-based, wholesale long-distance...

...result of new
information, future events, or otherwise. Forward looking statements are
inherently subject to **risks** and uncertainties, some of which cannot be
predicted or quantified. Future events and actual results...

...materially from those set forth in, contemplated by, or underlying the
forward-looking statements. The **risks** and uncertainties to which
forward-looking statements are subject include, but are not limited to, the
effect of government regulation, competition and other **risks** detailed
from
time to time in the Company's filings with the Securities and Exchange...

20/3,K/5 (Item 5 from file: 613)
DIALOG(R)File 613:PR Newswire
(c) 2005 PR Newswire Association Inc. All rts. reserv.

00201305 19991025DCM039 (USE FORMAT 7 FOR FULLTEXT)
**INFe.com Announces Deal with Intelligent Systems, Inc.; Intelligent Systems
Finalizes Consulting Agreement with INFe.com**
PR Newswire
Monday, October 25, 1999 11:23 EDT
JOURNAL CODE: PR LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE

WORD COUNT: 404

TEXT:

...server software applications for nearly a decade. Their flagship product iRAVES(TM) (Internet Real-Time **Address Verification** Enterprise System), is an **internet** -based **transaction** service bureau that can be integrated as part of any existing e-commerce application. ISI...

...Service's proprietary database to provide users with a valuable data integrity tool that instantly **validates** any United States **address**market potential," said Thomas Richfield, President and CEO of INFe.com. "The need to perform **address verification** for e-commerce companies is critical, because misdelivered and returned products result in millions of...

...product time to market by saving time and eliminating error, and most importantly, reduces the **risk** of **fraud** . These are absolutely vital functions for any Web site or e-commerce application and the iRAVES makes it very easy to incorporate."

INFe.com provides INFeStructure(TM) for **electronic commerce** and internet-based companies by providing our clients with their most needed resources of funding...

20/3,K/6 (Item 6 from file: 613)

DIALOG(R)File 613:PR Newswire

(c) 2005 PR Newswire Association Inc. All rts. reserv.

00195208 19991015LAF029 (USE FORMAT 7 FOR FULLTEXT)

Escrow.com Serves up Solution to Internet Fraud

PR Newswire

Friday, October 15, 1999 08:00 EDT

JOURNAL CODE: PR LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT

DOCUMENT TYPE: NEWSWIRE

WORD COUNT: 837

Escrow.com Serves up Solution to Internet Fraud

TEXT:

...com(TM), Inc., a comprehensive e-commerce solution that protects both buyers and sellers against **fraud** . The company plans to launch the site in the 1999 fourth quarter.

When launched, Escrow...

...com President and Chief Operating Officer Mark Attaway. "Our research shows that 72 percent of **online shoppers** would be

converted to online buyers if they were assured that the transaction would be totally safe. We're bringing security to **online purchasing** in a way that will make buyers and sellers more amenable to expanding how they...

...The site's products and services will include:

- Escrow services for auctions, classified and other **Internet**-enabled **transactions** ;
- Master-merchant transaction services for all forms of portal and **Internet commerce** ;
- **Shipping , authentication ,** appraisal and financing services.

The Escrow.com software will use "point and click" technology, allowing ...
...escrow on the Internet."

The Escrow.com site is being launched at a time when **Internet transaction** growth is expected to explode. According to a recent Forrester Research report, online business-to...

...result of new information, future events, or otherwise. Forward-looking statements are inherently subject to **risks** and uncertainties, some of which cannot be predicted or quantified. Future events and actual results...

...materially from those set forth in, contemplated by, or underlying the forward-looking statements. The **risks** and uncertainties to which forward-looking statements are subject include, but are not limited to, the effect of government regulation, competition and other **risks** detailed from time to time in the Company's filings with the Securities and Exchange...

20/3,K/7 (Item 7 from file: 613)
DIALOG(R)File 613:PR Newswire
(c) 2005 PR Newswire Association Inc. All rts. reserv.

00192448 19991012SFTU054 (USE FORMAT 7 FOR FULLTEXT)
CyberSource(R) and AGENCY.COM Form Alliance to Provide Online Merchants With Back-End eCommerce Services
PR Newswire
Tuesday, October 12, 1999 08:00 EDT
JOURNAL CODE: PR LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 613

TEXT:
...a complete suite of Internet eCommerce services, including Credit Card Payment services, the CyberSource Internet **Fraud** Screen enhanced by Visa, Tax Calculation, Distribution Control and Fulfillment Management services.

...By outsourcing eCommerce transaction services,

companies can focus on building their online businesses."

About CyberSource **Internet Commerce Suite**

The CyberSource **Internet Commerce Suite(SM)** is a robust set of real-time eCommerce transaction services that enable merchants to automate commerce operations, gaining the benefits of outsourcing complex **Internet commerce transaction** infrastructure while maintaining flexibility and control. Through software installed on a commerce server, merchants remotely access all CyberSource services, including: Credit Card Services, Tax Calculation, Internet **Fraud** Screen enhanced by Visa, Fulfillment Messaging, Delivery **Address Verification**, Digital Delivery, Digital Warehousing, Policy Compliance and Export Compliance.

About AGENCY.COM
AGENCY.COM is...

...developer and provider of eCommerce transaction services, and a pioneer in the area of Internet **fraud** detection. More than 600 Internet merchants in more than 26 countries have chosen to use CyberSource services. CyberSource provides mission-critical reliability with the CyberSource **Internet Commerce Suite(SM)**, offering merchant-controlled, real-time services including Payment Services, Tax Services, **Risk Management** Services, Distribution Control Services, and Fulfillment Management Services. Customers of CyberSource include leading Internet...
...cybersource.com or ir@cybersource.com.

NOTE: CyberSource is a U.S. registered trademark. CyberSource **Internet Commerce Suite** is a service mark of CyberSource Corporation. All other brands and product names are...

...COMPANY NAMES: **RISK MANAGEMENT**

20/3,K/8 (Item 8 from file: 613)
DIALOG(R)File 613:PR Newswire
(c) 2005 PR Newswire Association Inc. All rts. reserv.

00188796 19991005SFTU167 (USE FORMAT 7 FOR FULLTEXT)
Inabyte Introduces InaEmailCheck; Active-X Component Instantly Tests Status of Email Addresses
PR Newswire
Tuesday, October 5, 1999 17:26 EDT
JOURNAL CODE: PR LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 442

TEXT:
...for the Win32(R) architecture, today released an Active-X component

that immediately tests and **verifies** email **addresses** . InaEmailCheck is a valuable tool for e-commerce providers and other web-based businesses that need to **confirm** the validity of email **addresses** in order to complete mass mailings or execute **online transactions** . InaEmailCheck can be embedded directly into a web site, making it possible to test email...

...as a standalone utility. Companies that maintain large-scale email databases can use InaEmailCheck to **verify** and cull **addresses** on their lists quickly and efficiently. InaEmailCheck can also be used to **verify addresses** before a mass mailing, saving time and minimizing bounce-backs.

"For e-commerce companies and...

...as telephone numbers," said Mark Hennessy, president of Inabyte. "InaEmailCheck enables the immediate assessment and **verification** of virtually any email **address** . It's an efficient tool for keeping email databases up to date. Plus, by having the ability to **determine** the status of a **potential** customer's email address, online companies can cut down on input errors, improve communications and reduce the likelihood of **fraud** ."

20/3,K/9 (Item 9 from file: 613)
DIALOG(R)File 613:PR Newswire
(c) 2005 PR Newswire Association Inc. All rts. reserv.

00187498 19991004HSM048 (USE FORMAT 7 FOR FULLTEXT)
CyberSource(R) Extends Support for Next Generation INTERSHOP eCommerce Software
PR Newswire
Monday, October 4, 1999 09:30 EDT
JOURNAL CODE: PR LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 480

TEXT:
...reliable, scalable, real-time, transaction services to the INTERSHOP platform, including credit card processing, Internet **fraud** screening, tax calculation, delivery **address verification** and more. Such integration provides INTERSHOP users with a complete transaction solution, and allows them...

...developer and provider of eCommerce transaction services, and a pioneer in the area of Internet **fraud** detection. More than 600 Internet merchants in more than 26 countries have chosen to use CyberSource services. CyberSource provides mission-critical reliability with the CyberSource **Internet Commerce Suite(SM)**, offering merchant-controlled, real-time services including Payment Services, Tax Services, **Risk Management**

Services, Distribution Control Services, and Fulfillment Management Services.
Customers of CyberSource include leading Internet...

...info@cybersource.com or ir@cybersource.com

CyberSource is a U.S. registered trademark. CyberSource **Internet Commerce** Suite is a service mark of CyberSource Corporation. All other brands and product names are...

...COMPANY NAMES: **RISK** MANAGEMENT

20/3,K/10 (Item 10 from file: 613)
DIALOG(R)File 613:PR Newswire
(c) 2005 PR Newswire Association Inc. All rts. reserv.

00176224 19990914SFTU059 (USE FORMAT 7 FOR FULLTEXT)
CyberSource(R) Powers Online College Bookstore, eCampus.com
PR Newswire
Tuesday, September 14, 1999 08:01 EDT
JOURNAL CODE: PR LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 581

TEXT:

...leading provider of eCommerce transaction services today announced that eCampus.com has implemented the CyberSource **Internet Commerce** Suite(SM) to power its three million item college bookstore.

(Photo: <http://www.newscom.com...>

...has implemented real-time CyberSource eCommerce transaction services including, CyberSource Credit Card Processing, CyberSource **Internet Fraud** Screen and CyberSource Delivery **Address Verification** to ensure its customers a seamless, trouble-free buying experience.

About eCampus
ecampus.com is...

...at <http://www.ecampus.com> .

About CyberSource
CyberSource is a leading developer and provider of **Internet commerce** services. More than 600 Internet merchants worldwide have chosen to use CyberSource services. CyberSource provides mission-critical reliability with the CyberSource **Internet Commerce** Suite(SM) offering merchant-controlled, real-time services including Payment Services, Tax Services, **Risk** Management Services, Distribution Control Services, and Fulfillment Management Services.
Customers of CyberSource include Beyond.com...

...at <http://www.cybersource.com>

NOTE: CyberSource is a U.S. registered trademark. The CyberSource Internet Commerce Suite is a service mark of CyberSource Corporation. All other brands and product names are...

...COMPANY NAMES: RISK MANAGEMENT

20/3,K/11 (Item 11 from file: 613)
DIALOG(R)File 613:PR Newswire
(c) 2005 PR Newswire Association Inc. All rts. reserv.

00174064 19990907SFTU095 (USE FORMAT 7 FOR FULLTEXT)
Department of Consumer Affairs: Back to School Internet Tips for Kids (And Parents)
PR Newswire
Tuesday, September 7, 1999 14:02 EDT
JOURNAL CODE: PR LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 1,442

TEXT:

...But, as is the case with most amazing new technologies, the benefits are not without risks .

...or other interactive sites. And, with more and more opportunities to purchase goods and services online , cyber- shoppers need to take precautions to protect their personal and credit information and to ensure that...

...kids from accessing adult-oriented sites.

Golden Rule #3: Don't put anything in your electronic shopping cart until an adult checks it out!

Internet shopping is quick, easy and convenient -- if you make sure that you're dealing with legitimate businesses. Parents should instruct their kids to answer these questions before making online purchases : Did you get permission first? Do you know about the company you're buying from...

...reputation with the Better Business Bureau, the company's state attorney general, or the National Fraud Information Center at www. fraud .org or 800-876-7060.

-- Find out where the company is physically located. Resolving problems ...

...Attorney General's office in the company's home state. Or check with the National Fraud Information Center at www. fraud .org or 800-876-7060. But keep in mind that fraudulent companies come and go quickly, especially in cyberspace, so lack of a complaint record is...should comply with industry security standards, such as secure sockets layer (SSL) or set secure electronic transaction . These

standards "encrypt" or scramble the purchase information you send over the Internet, ensuring the...

...anyone.

-- Don't disclose personal information -- such as your address, telephone number, or e-mail **address** -- until you **check** the company's privacy policy to find out what it does with the information it...

...INDUSTRY NAMES: **ELECTRONIC COMMERCE** ;

20/3,K/12 (Item 12 from file: 613)
DIALOG(R)File 613:PR Newswire
(c) 2005 PR Newswire Association Inc. All rts. reserv.

00167671 19990824SFTU043 (USE FORMAT 7 FOR FULLTEXT)
CyberSource(R) Powers Internet Pharmacy, Rx.com
PR Newswire
Tuesday, August 24, 1999 08:00 EDT
JOURNAL CODE: PR LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 477

TEXT:

...developer and provider of real-time eCommerce transaction services, today announced that Rx.com, an **Internet retail** pharmacy, has selected CyberSource to power its real-time credit card transactions while significantly reducing **fraud** losses.

(Photo: <http://www.newscom.com/cgi-bin/prnh/19990513/CYBRSOURCELOGO>)
"We simply didn't..."

...Rx.com.

"We have great confidence in CyberSource's ability to minimize our exposure to **fraudulent** transactions and to provide superior services for our customers."

...said William Donahoo, VP of Marketing at CyberSource. "By outsourcing real-time payment services and **fraud** protection to us, they can concentrate on what they know best -- helping their customers lead...

...reminders via email; and maintain personal healthcare information.

On the Rx.com site, CyberSource Internet **Fraud** Screen is used in conjunction with CyberSource Credit Card Processing and Delivery **Address Verification** services to provide fast, convenient and fully automated payment services.

About CyberSource

CyberSource is a leading developer and provider of **Internet commerce** services. More than 600 Internet merchants worldwide have chosen to use CyberSource services. CyberSource provides mission-critical reliability

with
the CyberSource **Internet Commerce Suite**(SM) offering
merchant-controlled,
real-time services including Payment Services, Tax Services, **Risk**
Management
Services, Distribution Control Services, and Fulfillment Management
Services.
Customers of CyberSource include Beyond.com...

...email to
info@cybersource.com.

NOTE: CyberSource is a U.S. registered trademark. The CyberSource
Internet Commerce Suite is a service mark of CyberSource Corporation.
All
other brands and product names are...

...COMPANY NAMES: **RISK MANAGEMENT**

20/3,K/13 (Item 13 from file: 613)
DIALOG(R)File 613:PR Newswire
(c) 2005 PR Newswire Association Inc. All rts. reserv.

00167108 19990823HSM003 (USE FORMAT 7 FOR FULLTEXT)
TeleCheck Offers Next Generation Point-of-Sale Terminal
PR Newswire
Monday, August 23, 1999 08:59 EDT
JOURNAL CODE: PR LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 964

TEXT:

...cards, is
the first integrated payment terminal to securely, conveniently and
economically capture name and **address** information from a **check** .
Eclipse reads
the check MICR line (the bank numbers in magnetic ink along the bottom...

...check is handed
back to the consumer at the point of sale. Imaging reduces check **fraud** ,
improves collection efforts on bad checks and eliminates the need for
consumers to show driver...

...or other identification in most cases.

"With Eclipse, TeleCheck continues to lead the way in **electronic**
check
commerce and payment processing. Not only is TeleCheck the first to
introduce
a retail payment terminal...

...time as a traditional paper check.
In addition, since the check writer keeps the physical **check** , the **risk**
of
name, **address** and other personal information being used **fraudulently** is
substantially reduced.

For additional information on Eclipse, including photo, check
TeleCheck's

web site...

...210,000 retail, financial institution, grocery and other industry clients to increase their profitability, reduce risk and streamline operations. TeleCheck's check acceptance and **electronic commerce** solutions help businesses safely and efficiently accept payment at the point of sale, by telephone...

...http://www.telecheck.com .

Atlanta-based First Data Corp. is a leader in payment services, **electronic commerce** and **transaction** management products and services. First Data and its principal operating units process the information that...

...INDUSTRY NAMES: **ELECTRONIC COMMERCE** ;

20/3,K/14 (Item 14 from file: 613)
DIALOG(R)File 613:PR Newswire
(c) 2005 PR Newswire Association Inc. All rts. reserv.

00148593 19990721SFW004 (USE FORMAT 7 FOR FULLTEXT)
CyberSource(R) Announces Support for Allaire Spectra
PR Newswire
Wednesday, July 21, 1999 09:16 EDT
JOURNAL CODE: PR LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 585

TEXT:

...Internet-centric businesses that unite content, commerce, and customer interaction management. Together with the CyberSource **Internet Commerce Suite(SM)** of transaction services, Allaire Spectra delivers a powerful solution for developers and merchants...

...commerce-enabled Websites.

(Photo: <http://www.newscom.com/cgi-bin/prnh/19990513/CYBRSOURCELOGO>)
The CyberSource **Internet Commerce Suite** brings reliable, scalable, real-time transaction services to the Allaire Spectra platform, including credit card processing, **fraud** screening, tax calculation, and delivery **address verification** . As a result, developers and merchants can now build and deploy complete, fully automated, commerce...

...vendor," said Erna Arnesen, Vice President of Channels and Partners for CyberSource. "Since the CyberSource **Internet Commerce Suite** is pre-integrated into Allaire Spectra, we reduce the time and cost of integrating...

...web application platform vendors -- Allaire."

About CyberSource

CyberSource is a leading developer and provider of **Internet commerce** services. More than 400 Internet merchants worldwide have chosen to use CyberSource services. CyberSource provides mission-critical reliability with the CyberSource **Internet Commerce Suite**(SM) offering merchant-controlled, real-time services, including Payment Services, Tax Services, **Risk Management** Services, Distribution Control Services, and Fulfillment Management Services. Customers of CyberSource include Beyond.com...
...com, or email to
info@cybersource.com .

This release contains forward-looking statements that contain **risks** and uncertainties -- for example, unforeseen delays in product delivery. These statements may differ materially from...

...with the SEC, specifically the Registration Statement on Form S-1, which identifies other important **risk** factors.

NOTE: CyberSource is an U.S. registered trademark. CyberSource **Internet Commerce Suite** is a service mark of CyberSource Corporation. All other brands and product names are...

...COMPANY NAMES: **RISK MANAGEMENT**

20/3,K/15 (Item 15 from file: 613)
DIALOG(R)File 613:PR Newswire
(c) 2005 PR Newswire Association Inc. All rts. reserv.

00147662 19990720SFTU118 (USE FORMAT 7 FOR FULLTEXT)
Cybersource(R) Announces Second Quarter Financial Results
PR Newswire
Tuesday, July 20, 1999 16:15 EDT
JOURNAL CODE: PR LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 1,147

...and revenue was the addition of over 150 new Internet merchants that have chosen our **Internet Commerce Suite**. CyberSource merchant acquisition was strong across all eCommerce categories, including consumer electronics, apparel and...

...more companies realize the value that our services add to their eCommerce business. Our proprietary **risk** management service alone has helped our merchants save significantly in what would have been **fraudulent** transactions.

"We also strengthened our worldwide market position by adding a number of key eCommerce...

...a leading developer and provider of real-time e-commerce transaction services. Through its CyberSource **Internet Commerce Suite**, it offers services to online merchants for global payment processing, **fraud** prevention, tax calculation, export compliance, territory management, delivery **address verification** and fulfillment management. More than 500 merchants have chosen to use CyberSource services. CyberSource's...

...on the company's current expectations, and are subject to a number of uncertainties and **risks**. The company's actual results may differ materially. The uncertainties and **risks** include the pace of growth of eCommerce, the development by the company and its competitors...

...Securities and Exchange Commission, specifically the Registration Statement on Form S-1, which identifies important **risk** factors.

For more information visit <http://www.cybersource.com>, or email to info@cybersource.com or ir@cybersource.com.

NOTE: CyberSource is a U.S. registered trademark. CyberSource **Internet Commerce Suite** is a service mark of CyberSource Corporation. All other brands and product names are...

20/3,K/16 (Item 16 from file: 613)
DIALOG(R)File 613:PR Newswire
(c) 2005 PR Newswire Association Inc. All rts. reserv.

00117606 19990601ATTU008 (USE FORMAT 7 FOR FULLTEXT)
Sun-Netscape Alliance and Equifax Secure Announce Plans to Provide Advanced E-Commerce Security
PR Newswire
Tuesday, June 1, 1999 08:02 EDT
JOURNAL CODE: PR LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 1,620

TEXT:
...online identity authentication and digital credentialing services for companies wanting to rapidly deploy high-assurance **online commerce** applications. Under the agreement, Equifax Secure will use Netscape(R) Directory for Secure E-Commerce...

...and seller identities beyond traditional methods such as Social Security number, driver's license and **address**. The **authentication** service will also enable new customers to more easily sign up online for sensitive services...

...to e-commerce
but also accelerate the use and acceptance of online business, such as
online
trading, banking, **shopping**, auctions, and others."

"Whether e-commerce businesses deploy their own directory,
authentication
and certificate services...

...manager of Equifax Secure Inc.
"By using more advanced authentication measures, companies will reduce the
risk of identity **fraud** and help increase their customers' confidence in
e-commerce."

Accelerating the use and acceptance of the **Internet** for e- **commerce**
requires establishing new levels of individual and enterprise privacy and
security in networked environments. According...

...Equifax Secure's unique authentication and Netscape's
Directory Server and Certificate Management System allows **electronic**
commerce
and extranet sites to issue digital certificates with much greater
assurance
of the identity of...

...process to Equifax Secure, including the issuing, and registration of
new
certificates. By reducing the **risk** of **fraud** at the point where
certificates
are issued, this technology increases the practical uses and value...

...combination of strong
technical infrastructure products with established and trusted assurance
services significantly reduces the **risk** of managing dynamic business
relationships on the Internet."

The Equifax Secure authentication module will be...

...commerce over the
Internet and other networks. Equifax Secure e-commerce solutions
significantly reduce the **risk**, cost and complexity of assuring the
privacy and
security of **electronic transactions** and are available for companies
across a
wide range of industries.

Equifax (www.equifax.com...

...INDUSTRY NAMES: **ELECTRONIC COMMERCE** ;

20/3,K/17 (Item 17 from file: 613)
DIALOG(R)File 613:PR Newswire
(c) 2005 PR Newswire Association Inc. All rts. reserv.
00102373 19990504SFTU062 (USE FORMAT 7 FOR FULLTEXT)
**Heartland Payment Systems and CyberSource(R) Debut One-Stop E-Commerce
Payment Solution**
PR Newswire
Tuesday, May 4, 1999 13:10 EDT
JOURNAL CODE: PR LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE

WORD COUNT: 686

...stop online credit card processing solution for eCommerce merchants," said John Waldron, Vice President of **Internet Marketing and Sales** for HPS. "The combination of CyberSource services and HPS' 48-hour online merchant account application...

...channel sales at CyberSource. "CyberSource eTransaction services cover the full range of eCommerce functions, from **fraud** screening to delivery **address verification**, and are all available to merchants taking advantage of this new one-stop program."

Once...

...services at any time, without integrating additional software. These other services include CyberSource IVS(TM) **Fraud** Screen for managing the **risk** of credit card **fraud** and CyberSource SmartCert(TM) for digital delivery, as well as CyberSource services for automatic sales tax/VAT calculation, delivery **address verification**, fulfillment messaging, export control and global rights registry.

Becoming an HPS VAR
Companies interested in...

...service merchant card processor (for credit, debit, ATM, and check cards), handling services that include **fraud** monitoring, reconciliation, compensation, ACHing of merchant funds, draft retrieval processing, and chargeback processing. HPS conducts...

...buttons of over 400 Internet merchants worldwide, CyberSource provides mission-critical reliability with the CyberSource **Internet Commerce** Suite offering merchant-controlled, real-time services including tax services, payment services, **risk** management services, export control services, policy control services, fulfillment messaging, delivery **address verification** and secure digital delivery. Cybersource's customers include Beyond.com, BUY.COM, Compaq Computer, Egghead...

...INDUSTRY NAMES: **ELECTRONIC COMMERCE** ;

20/3,K/18 (Item 18 from file: 613)
DIALOG(R)File 613:PR Newswire
(c) 2005 PR Newswire Association Inc. All rts. reserv.

00102361 19990504SFTU063 (USE FORMAT 7 FOR FULLTEXT)
NetCommerce Holdings and CyberSource(R) Partner to Bring eCommerce To Andean Pact Countries
PR Newswire

Tuesday, May 4, 1999 13:00 EDT

JOURNAL CODE: PR LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT

DOCUMENT TYPE: NEWSWIRE

WORD COUNT: 694

TEXT:

...in the Andean Pact countries with flexible and cost-effective solutions for global payment processing, **fraud** prevention, tax calculation, export compliance, territory management, delivery **address verification** and fulfillment management. Accessed remotely on an "on-demand, pay-per-transaction" basis, CyberSource eCommerce transaction services enable online merchants to outsource the full suite of **electronic commerce** functionality, and avoid having to build their own complex and expensive transaction processing infrastructures.
"NetCommerce...

...payment gateway to process credit card payments in real-time, and CyberSource's IVS(TM) **Fraud** Screen to protect themselves automatically against costly credit card **fraud**. GeoPay enables merchants to accept payments in multiple national currencies, thus extending their base of...

...eTransaction Suite integrates seamlessly with merchants' online store platforms. In addition to GeoPay and IVS **Fraud** Screen services, NetCommerce's customers will be able to take advantage as needed of additional...

...services without integrating additional software. These other services include digital delivery of software and other **electronic** content, automatic **sales tax/ VAT**, export control and territory management, and global rights management.

About CyberSource

CyberSource is...

...buttons of over 400 Internet merchants worldwide, CyberSource provides mission-critical reliability with the CyberSource **Internet Commerce** Suite offering merchant-controlled, real-time services including tax services, payment services, **risk** management services, export control services, policy control services, fulfillment messaging, delivery **address verification** and secure digital delivery. Cybersource's customers include Beyond.com, BUY.COM, Compaq Computer, Egghead...

...NetCommerce Holdings, Inc. was formed to exploit the growing business opportunities in Latin America for **Electronic Commerce** services. The company strategy is to select "best-of-breed" solutions and offer them to...

...billing. NetCommerce's first provider is CyberSource Corp., a leader in global payment processing, anti- **fraud**, digital delivery and fulfillment services. NetCommerce is a spin-off of NetHosting, C.A., founded...

...INDUSTRY NAMES: **ELECTRONIC COMMERCE** ;

20/3,K/19 (Item 1 from file: 813)
DIALOG(R)File 813:PR Newswire
(c) 1999 PR Newswire Association Inc. All rts. reserv.

1464922 NETH029
ICOMS is Selected for MasterCard Shop Smart!(TM) Program to Assure Safe Transaction Processing Over Internet

DATE: April 29, 1999 12:57 EDT WORD COUNT: 635

, April 29 /PRNewswire/ -- ICOMS (**Internet Commerce** Services Corp.) has been selected by MasterCard as a commerce services provider which utilizes the...

...circuits;

-- Credit card numbers are immediately moved off-line onto a secure server;

-- Buyers are **authenticated** through an **address verification** system;

ICOMS qualifies merchants before agreeing to provide the MerchantTrax service to avoid working with sites at high- **risk** to **fraud**.

"ICOMS has put in place the 'best practices' required by MasterCard, including comprehensive security systems...

... forward to working with ICOMS to enroll their merchants in MasterCard Shop Smart!"

About ICOMS

Internet Commerce Services Corporation (ICOMS) is a leading independent outsource provider of **Internet commerce transaction** services, providing order management and payment processing services to more than 200 clients. ICOMS has...

...and Hot Deals are trademarks of MasterCard International Incorporated.

ICOMS and MerchantTrax are trademarks of **Internet Commerce** Services Corporation.

Other product and company names are the property of their respective owners.

SOURCE **Internet Commerce** Services Corp.
COMPANY NAME: **INTERNET COMMERCE** SERVICES CORP. (ICOMS...

20/3,K/20 (Item 2 from file: 813)
DIALOG(R)File 813:PR Newswire
(c) 1999 PR Newswire Association Inc. All rts. reserv.

1461426 LAM016
Verio Takes E-Commerce Global with Multi-Currency Solutions from CyberSource

DATE: April 26, 1999

08:15 EDT

WORD COUNT: 1,054

... agreement with CyberSource(R), a leading supplier of e-commerce transaction services, to offer international **electronic commerce** solutions capable of processing and settling **on - line transactions** in 29 currencies. Under the agreement, Verio will resell CyberSource's multi-currency payment processing...

... Web-hosting services to provide a comprehensive e-commerce solution for the burgeoning international marketplace. " **Internet commerce** will grow from \$50.4 billion worldwide in 1998 to more than \$1.3 trillion...

... in regions outside of the United States accounts for just 26 percent of the total **Internet commerce** market in 1998, that number will increase to 46 percent by 2003, totaling \$610 billion...

... largest Web-hosting company, Verio is playing a critical role in the international growth of **electronic commerce** ," said Tony Bates, executive vice president and international general manager of CyberSource. "With its large...

... controlled, real-time services that go well beyond a payment gateway -- including global tax calculation, **fraud** screening, delivery **address verification** , export and territory management, fulfillment notification, and digital goods delivery. CyberSource's customers include Beyond...

...to compete in the new world of business: high-speed Internet access, Web site hosting, **electronic commerce** , virtual private networks, and other enhanced services. Verio supports its operations with a highly reliable...

... the Private Securities Litigation Reform Act of 1995. These forward-looking statements are subject to **risks** and uncertainties, including but not limited to fluctuations in operating results, additional capital requirements, competition... K filed on March 31, 1999, for a further discussion of Verio's business and **risk** factors that may affect operating and financial results.

SOURCE Verio Inc.

20/3,K/21 (Item 3 from file: 813)

DIALOG(R)File 813:PR Newswire

(c) 1999 PR Newswire Association Inc. All rts. reserv.

1405299

ATM005

Equifax Secure, Security First Network Bank Announce First Use of Next-Generation Authentication Technology

DATE: January 18, 1999

08:30 EST

WORD COUNT: 1,331

... Obtaining more complete and accurate identification through Equifax Secure assures the integrity and privacy of **electronic communications** and **transactions** from the beginning of the online relationship with new SFNB customers.

"We are delighted that...

... interactive query, 4) performs easily and seamlessly for the user, and 5) provides pattern recognition/ **fraud** detection.

JMB

Date: 27-Oct-05

The service can range in complexity from **verification** against **customer data**, to developing and hosting **authentication** models. More specifically, the service:

-- authenticates individuals, reducing the manual ID process to save time...Securities Litigation Reform Act of 1995 and the Securities Exchange Act of 1934. Future events, **risks** and uncertainties, individually or in the aggregate, could cause actual results to differ materially from...

...and U.S. economic conditions, changes in demand for the company's products and services, **risks** associated with the integration of acquisitions and other investments, and other factors discussed in the...

20/3,K/22 (Item 4 from file: 813)
DIALOG(R)File 813:PR Newswire
(c) 1999 PR Newswire Association Inc. All rts. reserv.

1404599 HSF003
eBay(TM) Selects Equifax Secure to Verify Identity of Buyers, Sellers Over the Internet

DATE: January 15, 1999 08:35 EST WORD COUNT: 894

...in knowing the identity of other users. Equifax Secure will help support this initiative by **verifying user identification information**."

Jeff Johnson, Equifax senior vice president and general manager of Equifax Secure, said, "We are...

...not access the Internet, saying that ensuring the privacy and security of personal data and **on-line transactions** would influence them to start using the Internet. According to Consumer Reports and the Computer Security Institute, millions of dollars are lost each year from identity **theft**, unauthorized insider access, **theft** of proprietary information, telecommunications and financial **fraud**, and other security breaches over public and private networks.

"The Equifax Secure authentication technology significantly reduces the **risk**, cost and complexity of assuring the privacy, integrity and security of **electronic communications and transactions** over the Internet," Johnson said. "Equifax Secure and eBay share a commitment to eliminating **fraud** through implementing safeguards on the **Internet** for e-commerce."

The authentication technology is part of a suite of e-commerce solutions developed by Equifax...

...Securities Litigation Reform Act of 1995 and the Securities Exchange Act of 1934. Future events, **risks** and uncertainties, individually or in the aggregate, could cause actual results to differ materially from...

...and U.S. economic conditions, changes in demand for the company's products and services, **risks** associated with the integration of acquisitions and other investments, and other factors discussed in the...

20/3,K/23 (Item 5 from file: 813)
DIALOG(R)File 813:PR Newswire

(c) 1999 PR Newswire Association Inc. All rts. reserv.

1356614

CGTU054

**PaylinX Announces Paymentech Payment Pipe for Microsoft Site Server 3.0,
Commerce Edition & Call Centers**

DATE: October 13, 1998

18:41 EDT

WORD COUNT: 564

... through the PaylinX platform, Paymentech clients can leverage real time credit card authorization functionality for **Internet transactions** while also complementing existing call center operations."

"Our relationship with PaylinX continues the expansion of...

... in the direct response electronic payments arena," said John Shirey, Paymentech's senior director of **electronic commerce**. "Together our companies deliver a true end-to-end solution that offers a low- **risk**, effective way to transform the Internet into a key distribution channel for direct marketers."

Offering PS2000 **address verification** compliance, PaylinX payment servers securely manage real time authorizations, settlements and reporting for conventional credit...

...000 transactions per hour via frame relay connectivity to the Paymentech network. Clients realize improved **fraud** control, reduced bad debt exposure and enhanced inventory turnover through the PaylinX-Paymentech solution set...

... are generally available and currently shipping. PaylinX Corporation is an innovator in the field of **electronic commerce** and the leader in enterprise payment servers. PaylinX software is available from PaylinX Value Added...

...R) is a registered trademark and PaylinX for Site Server, Payment Pipes, Processor Cartridges and "**Electronic Commerce** . Today." are trademarks of PaylinX Corporation. Other trademarks, service marks and copyrights are the property...

20/3,K/24 (Item 6 from file: 813)

DIALOG(R)File 813:PR Newswire

(c) 1999 PR Newswire Association Inc. All rts. reserv.

1343886

SFTU024

**CyberSource Announces CyberSource IVS 3.0. The Fraud Screen Providing the
Most Precise Protection From Internet Credit Card Fraud**

DATE: September 22, 1998

08:04 EDT

WORD COUNT: 1,046

**CyberSource Announces CyberSource IVS 3.0. The Fraud Screen Providing the
Most Precise Protection From Internet Credit Card Fraud**

Sept. 22 /PRNewswire/ -- Zeroing in on Internet credit card **fraud**, CyberSource(R) Corporation today introduced, at the **Internet Commerce Expo** in Los Angeles, the third release of its CyberSource IVS(TM) automated **fraud** screen application for Web merchants. Part of CyberSource's comprehensive suite of on-demand commerce...

... provides even finer, dynamic controls to help commercial Web sites maximize online profitability and control **fraud** to less than 1%.

Conventional **fraud** detection schemes, such as the **Address Verification Service (AVS)** which is only available for US cardholders, are largely ineffective in the anonymous environment of the Internet. While other emerging Internet **fraud** screen offerings tend to provide 'cookie-cutter' **risk** assessment methods that presume a similar profile for all merchants and product categories, CyberSource IVS 3.0 provides merchants with the industry's first dynamically controlled on-demand **fraud** screening application.

CyberSource IVS 3.0 enables merchants to customize a **fraud** screen unique to their business and specify the **risk** threshold they are willing to accept by product, or product category. The merchant may change...

...in ship-to-/bill-to address, and consumer email and IP addresses.

Using CyberSource IVS, **fraudulent** transactions, which account for approximately 21% of digital product orders and 15% of hard goods...

... credit card account status is in jeopardy of being revoked. Further, CyberSource IVS accurately assesses **fraud risk** before the order is consummated, which is far more cost-effective than dealing with **fraud** after it occurs. CyberSource IVS, which can be utilized in parallel with the credit card authorization process, uses data supplied with the order and artificial intelligence to " **score** " the potential **risk** of each transaction -- typically in less than five seconds.

"With digitally delivered products, you are potentially exposed to **fraud** on an alarming scale, yet CyberSource's IVS technology has allowed us to drop our credit card **fraud** rate from an unacceptable level to less than 1% of sales, virtually overnight," said Pamela Roberts director of **Internet sales** at Symantec. "The solution is so flexible that we are able to tweak any number of variables, such as assigning different levels of **risk** for differently priced products. CyberSource IVS 3.0 looks highly promising with its even more granular controls for avoiding of **fraud**."

"CyberSource IVS has gained acceptance as the premier mechanism for managing exposure to Internet credit card **fraud** and preserving the credit card statuses of Web merchants," said Steven Klebe, VP of Payment...

... merchant benefits from the collective experiences of other merchants to pinpoint the telltale signs of **fraud**. Manual checking methods, and proprietary single-merchant solutions, lack this benefit and, consequently, much of...

...IVS 3.0 enhancements

CyberSource IVS 3.0 enables a Web merchant to dynamically set **risk** assessment parameters to match their business needs. A merchant can set these parameters uniformly across...

... purchase hours" , transactions performed during the expected purchase hours (purchaser's location) are assigned no **risk** while transactions performed outside of expected purchase hours are applied a **risk score**.

Bill to/Ship to variance -- determines whether the geographic proximity of the ship-to and bill-to addresses should be a component of the CyberSource IVS **score** (accommodates products that are often purchased as gifts and shipped to an address other than...

... CyberSource on-demand commerce applications, businesses automate

operations and gain the benefits of outsourcing complex **Internet commerce** infrastructures, without giving up flexibility and control. Using messaging software installed on a commerce server...

...applications , including:

CyberSource GeoPay(TM) high-performance global payment processing gateway

CyberSource IVS(TM) Internet **fraud** screen
CyberSource GlobalTax(TM) real-time sales & VAT tax calculation

CyberSource TerritoryManager(TM) export compliance...

...time. Global, on-demand commerce applications include a high performance multi-currency payment gateway, Internet **fraud** screen, real-time export compliance and territory management, fulfillment messaging and digital delivery applications; as...

20/3,K/25 (Item 7 from file: 813)
DIALOG(R)File 813:PR Newswire
(c) 1999 PR Newswire Association Inc. All rts. reserv.

1343885 SFTU019
CyberSource and Paymentech Join Forces to Provide Robust Payment Capability and Attack Credit Card Fraud

DATE: September 22, 1998 08:04 EDT WORD COUNT: 1,183

CyberSource and Paymentech Join Forces to Provide Robust Payment Capability and Attack Credit Card Fraud

... a marketing agreement aimed at providing a robust payment processing capability that dramatically reduces the **risk** of Internet credit card **fraud** . The announcement was made at the **Internet Commerce Expo** in Los Angeles.

In referring its Internet merchants to CyberSource on-demand commerce applications(TM), including CyberSource GeoPay(TM) and CyberSource IVS(TM) **fraud** screen, Paymentech is expanding the **electronic commerce** options it affords its customers. CyberSource proactively helps commercial Web sites manage their exposure to **fraud** , in order to protect profits and preserve their critical ability to accept credit cards.

Credit card **fraud** on the Internet costs merchants both time and money -- time spent attempting to identify **fraudulent** transactions and dealing with **fraud** 's resulting chargebacks, and lost money from reduced profits, bank chargeback fees, and penalties imposed by credit card associations such as VISA and MasterCard. A consistently high level of **fraud** can even cause a card association to revoke a merchant's ability to take credit cards. While **Internet** merchants **selling** either physical goods or electronically downloadable products and services are both vulnerable, digital goods merchants are at particular **risk** because the goods are already "out the door" before a **fraudulent** transaction can even start to be detected by conventional means.

To combat this problem, Paymentech and CyberSource have teamed to offer Paymentech merchants the Internet's most comprehensive **fraud** screening technology. CyberSource IVS, the Internet **fraud** screen, uses a variety of techniques, including artificial intelligence, to verify the identity of

the purchaser and flag potentially **fraudulent** transactions before the order is consummated. Numerous characteristics of each order are automatically analyzed, and the order is then scored for its **fraud** potential. In addition, Paymentech has applied its own **fraud** -fighting experiences and techniques to CyberSource IVS in order to even further increase its effectiveness...

... have shown that Internet merchants using CyberSource IVS are able to manage their exposure to **fraudulent** transactions to less than 1% of their total orders.

"Our goal is to make our...

... a full, robust range of point-of-sale solutions," said John Shirey, senior director for **electronic commerce** at Paymentech. "Paymentech has long provided the best **fraud** prevention services to traditional direct marketers. In teaming with CyberSource, our Internet merchants can now be equipped with a high-value **fraud** fighting mechanism that significantly lowers direct and indirect costs."

Powerful anti- **fraud** technology for Internet merchants

Unlike single merchant solutions developed in-house or purchased as a ...

... weighted scores and compares those scores against a merchant's defined threshold. The higher the **score**, the higher the **risk** that the attempted transaction is **fraudulent**. With this approach, the merchant is able to decide the level of **risk** he wishes to accept. For example, a merchant can decide that a **score** of 25 or higher indicates an unacceptable **risk** for orders placed between midnight and 5:00 a.m., yet is acceptable during daylight hours.

"Traditional **fraud** detection mechanisms used for mail and telephone orders, such as the **address verification** service (AVS), simply aren't effective in the anonymous environment of the Internet," said Steve...

...president of Payment Industry Alliances at CyberSource. "CyberSource IVS goes a lot deeper than just **verifying addresses**. Rather, it examines a multitude of variables to spot the tell-tale footprints of identity **fraud** and to stop it before it impacts the merchant."

Robust payment processing

In addition to referring to CyberSource for **fraud** screening capabilities, Paymentech has added CyberSource GeoPay, the secure on-demand gateway to its menu...

... CyberSource on-demand commerce applications, businesses automate operations and gain the benefits of outsourcing complex **Internet commerce** infrastructures, without giving up flexibility and control. Using messaging software installed on a commerce server...

...applications, including:

CyberSource GeoPay(TM) high-performance global payment processing gateway

CyberSource IVS(TM) Internet **fraud** screen

CyberSource GlobalTax(TM) real-time sales & VAT tax calculation

CyberSource TerritoryManager(TM) export compliance...

...time. Global, on-demand commerce applications include a high performance multi-currency payment gateway, Internet **fraud** screen, real-time export compliance and territory management, fulfillment messaging and digital delivery applications; as...

20/3,K/26 (Item 8 from file: 813)
DIALOG(R)File 813:PR Newswire
(c) 1999 PR Newswire Association Inc. All rts. reserv.

1293932 DAW023
Electronic Check Acceptance Introduced Nationwide; The Power of the Check Without the Paper

DATE: June 17, 1998 12:04 EDT WORD COUNT: 990

...off the bottom of the check. The consumer simply signs a printed receipt authorizing the **electronic transaction**, and the paper check along with a copy of the authorization slip is returned to...

... bank statement for reconciliation purposes, and consumers retain the same rights as today in disputing **fraudulent** items posted to their account.

Consumer Benefits

Consumers continue to benefit from the float of...

... time as a traditional paper check. In addition, since the check writer keeps the physical **check**, the **risk** of name, **address** and other personal information being used **fraudulently** is substantially reduced.

Reconciling bank statements is easy, since ECA checks usually clear within two...

... the transaction, including merchant name, settlement date and amount, appears on the statement with other **electronic transactions**, such as direct payroll deposits or ATM transactions. Consumers wanting more information, or a consumer...

... leading providers of transaction processing services -- credit, debit and pre-paid card processing; payment systems; **electronic commerce** and information-based services to both businesses and consumers. In partnership with clients, primarily financial...

20/3,K/27 (Item 9 from file: 813)
DIALOG(R)File 813:PR Newswire
(c) 1999 PR Newswire Association Inc. All rts. reserv.

1135092 SFM057
CyberSource's Digital Commerce Services Attract Over 100 Merchants in First 100 Days

DATE: August 4, 1997 12:28 EDT WORD COUNT: 1,229

CyberSource's Digital Commerce Services Attract Over 100 Merchants in

First 100 Days

, Aug. 4 /PRNewswire/ -- CyberSource Corp., a pioneer in **digital goods commerce** services, today announced results related to the commercial introduction of its unique suite of **Internet commerce** services. In the first 100 days since the launch, over 100 merchants, publishers and resellers...

... signed agreements with CyberSource to support their Web-based product distribution strategies with mission-critical, **digital commerce** applications. Businesses are turning to CyberSource for its more than three years of experience in digital product distribution, as well as unique **Internet** -specific **transaction** and fulfillment services, including CyberSource's **fraud** screen and export control applications and trusted intellectual property rights management services.

More than 25...

...enables merchants to process transactions online in as little as a week.

"The challenges of **Internet commerce** are unique to the virtual world. By their very nature, many of these challenges require...

... maintain the totality of services we've developed over the last three years. By outsourcing **digital commerce** services to CyberSource, customers reduce time-to-market and can focus their efforts on the marketing of their sites, leaving the back office complexities of **digital commerce** to us."

"Outsourcing **electronic commerce** activities to CyberSource has given us the opportunity to provide our customers with a secure **electronic purchase** option while allowing us to stay focused on our core competencies in catalog sales, marketing...

... leading international direct marketer of software development products and tools for PCs, servers and networks.

Digital Commerce Challenges

While credit card processing and the physical fulfillment of an electronic order are relatively...

... present unique challenges. CyberSource has developed a suite of applications which addresses the complexities of **digital commerce** such as Internet credit card **fraud**, export control and intellectual property rights management. CyberSource customers have the ability to select the...

... to quickly acquire transaction capability and speed return on investment.

CyberSource's applications include:

Internet **fraud** screen. CyberSource's proprietary **fraud** screen, IVS(TM), uses the powerful combination of an artificial intelligence system and an extensive, dynamically-updated database to analyze transactions and reduce the **risk of fraud**.

Export control. This proprietary application addresses compliance with government restrictions on sales to an ever...

... experience indicates that businesses, especially those selling or distributing digital goods, do not realize the **risks** until it is too

late.

For example, traditional methods for addressing credit card **fraud** via bank authorization and **address verification** are not sufficient for web-based businesses. The anonymity offered by the Web, coupled with...

... ability to rapidly access multiple shopping sites, significantly increases the Internet merchant's exposure to **fraudulent** transactions. CyberSource's **fraud** screen, IVS(TM), uses a proprietary, artificial intelligence program that performs dozens of checks on the transaction, beyond real-time bank validation, to detect **fraud**. While Internet **fraud** is a problem many merchants face with no apparent solution, CyberSource's IVS(TM) has successfully reduced credit card **fraud** losses to as little as one half of one ... critical to Web-based merchants, who often are not aware of the prevalence of online **fraud** or that banks and credit card companies hold merchants liable for **fraudulent** purchases.

Another issue is a business' compliance with federal government restrictions prohibiting the sale of...
...provider of commerce services that support digital product distribution. These services include credit card processing, **fraud** screening, tax calculation, export control, secure digital goods distribution, a trusted electronic license clearinghouse, and...

20/3,K/28 (Item 10 from file: 813)
DIALOG(R)File 813:PR Newswire
(c) 1999 PR Newswire Association Inc. All rts. reserv.

1131419 CLM024
Metromail On-Line Services Improves Fraud Prevention with the Release of CheckPoint 2.0.

DATE: July 28, 1997 11:09 EDT WORD COUNT: 541

Metromail On-Line Services Improves Fraud Prevention with the Release of CheckPoint 2.0.

... Corporation (NYSE: ML), is announcing the release of version 2.0 of its CheckPoint(R) **address verification** and **fraud** prevention system.

"CheckPoint 2.0 uses leading edge, proprietary matching logic to **verify customer information** against a comprehensive compiled group of data sources to provide superior verification and **fraud** prevention capabilities," said Phil Bonello, Senior Vice President-General Manager, On-Line Services. "Besides updating...

... options, access to both summary and detail information related to requested searches, and an automated **risk** scoring and decision system."

CheckPoint 2.0 features address standardization and zip + 4 coding, change of address disclosure, address type coding (residential, business, seasonal, etc.), address deliverability designation, high **risk** address notification, phone number designation (residential, business, cellular, pager, etc.), customer demographic verification, home-ownership...

... acceptance purposes. The detail page will display the matched and unmatched search options.

According to On - Line Services Marketing Manager Chuck Sokolich, CheckPoint 2.0 incorporates customer-driven product improvements. "After

canvassing our customers...

... flagging potential manipulations of information on credit and insurance applications before they are approved, certifying **Internet transactions**, and maximizing the effectiveness of credit bureau searches.

On-Line Services, a division of Metromail...

20/3,K/29 (Item 11 from file: 813)
DIALOG(R)File 813:PR Newswire
(c) 1999 PR Newswire Association Inc. All rts. reserv.

1066249 LAM047
CyberSource Stops Over \$1 Million Dollars in Online Fraud

DATE: March 10, 1997 08:04 EST WORD COUNT: 571

CyberSource Stops Over \$1 Million Dollars in Online Fraud

, March 10 /PRNewswire/ -- CyberSource Corp., a leading **Internet commerce** services provider, today announced that their breakthrough IVS(TM) **Fraud** Screen technology saved Web store owners over \$1 million dollars in online **fraud** in the final half of 1996.

Research by CyberSource shows that electronically delivered goods are significantly more susceptible to **fraudulent** purchases than physically delivered goods. Because Internet Service Providers (such as AOL) are targets of credit card **fraud** too, it is simple for criminals to set up fictional identities using temporary e-mail...

... the virtual world, and no physical address is required for delivery, which is why the **risk** for online consumers and Web merchants is much greater.

Arresting Online Bandits

CyberSource's experience with online **fraud** is that the computerized nature of **online transactions** allows criminals to automate credit card **fraud** -- facilitating multiple attempts. Most recently, CyberSource joined forces with local law enforcement agencies in Modesto, California and Green Bay, Wisconsin to pursue individuals attempting **fraudulent** purchases. Both cases resulted in the culprits being arrested. CyberSource has also been successful tracking down international online criminals in Poland and Israel, where credit card **fraud** is prevalent. However, local law enforcement bodies generally do not have adequate staff power to...

... the Internet as 'beyond their jurisdiction'. The Secret Service, which is responsible for pursuing wire **fraud**, does not have resources to seriously address this problem on such a large scale.

Extra Layer of Security

CyberSource's comprehensive database of recorded **fraudulent** activity is continuously aggregating information about online criminals that attempt to use make-believe or...

...an extra layer of security for online consumers and merchants with their proven IVS(TM) **Fraud** Screen technology, which goes far beyond the protection any financial institution's simple **address verification** system currently offers.

IVS(TM) **Fraud** Screen

CyberSource's proven **fraud** technology is based on a combination of artificial intelligence (AI) code developed by CyberSource and a knowledge base of hundreds of thousands of **online transactions** it has processed. Every credit card transaction is validated by an authorized financial institution in...

... CyberSource's own AI software that reviews more than 100 validation factors to uncover potential **fraud**. Once the credit card information has been validated by both systems, an order is cleared for delivery.

About CyberSource

CyberSource Corp. is a leading **Internet commerce** service provider specializing in turn-key, backoffice **Internet Commerce Services (ICS)** that include: real-time credit card transaction processing, IVS **Fraud** Screen, export control, sales tax tables, secure electronic fulfillment and EDI. For the past two...

...the CyberSource Web site at www.cybersource.com or call 408-556-9100.

IVS(TM) **Fraud** Screen is a registered trade mark of CyberSource Corporation

SOURCE CyberSource Corp.

20/3,K/30 (Item 12 from file: 813)
DIALOG(R)File 813:PR Newswire
(c) 1999 PR Newswire Association Inc. All rts. reserv.

1056853 DCF002
Bank of Montreal First to Offer Instant Approvals For Mortgages Over the Internet

DATE: February 14, 1997 10:01 EST WORD COUNT: 741

...the Internet, Bank of Montreal has taken aggressive steps to protect its customers against data **fraud** and potential loss of confidential information. All mortgage applications must pass several security checks as ...

... application information is valid. Once the application is sent to the mortgage origination system, the **customer information** is re-verified. The system prompts the customer when completing the applications, pointing out any mistakes in the...

... home page" on the World Wide Web. "True Internet banking is the ability to offer **online**, real-time **transaction** processing and credit decisions," said Charles O. Rossotti, chairman of AMS. "Bank of Montreal is ...

...support engine, Strata, takes customer information and scores it against the Bank's pre-defined **risk** levels, based on customer profiles and credit policy. Using this information, the Bank then makes...

20/3,K/31 (Item 13 from file: 813)
DIALOG(R)File 813:PR Newswire
(c) 1999 PR Newswire Association Inc. All rts. reserv.

0946031

SFM022

**CYBERSOURCE UNVEILS FIRST MULTI-TIER ELECTRONIC DISTRIBUTION MODEL,
SUPPORTS MICROSOFT STANDARDS**

DATE: May 6, 1996

15:35 EDT

WORD COUNT: 1,003

...PRNewswire/ -- CyberSource Corp., the leading Internet electronic software distribution company, announced today the availability of **Internet Commerce Services (ICS)** for a new multi-tier electronic distribution model. CyberSource, supporting the open Microsoft...

...entire industry -- publishers, distributors, resellers and other channel partners -- a broad range of turn-key **electronic transaction** processing and distribution services.

Merisel has announced its intent to work with CyberSource to facilitate...

...over the Internet. These companies are leveraging CyberSource's experience in, and technology for secure **electronic** distribution and **transaction** processing. CyberSource has been distributing software electronically since 1994 when it launched software.net(TM...

...software superstore specializing in electronic distribution.

"CyberSource provides a comprehensive, secure and scalable solution to **electronic transactions** and software distribution over the Internet," said Johan Liedgren, director of channel policies for Microsoft...

...distributors to sell to a wide range of resellers. Alternatively, ICS provides complete back-office **electronic commerce** services for companies that wish to sell direct or use a single-tier distribution model...

...are used to unlock and open a digitally encrypted container which contains the software for **electronic** distribution.

Distributor **Commerce** Services which facilitate online distribution of both physical and digital products by providing online, real...

...Services.

Merchant Commerce Services which provide a secure yet simple system for processing and managing **Internet commerce transactions**. With Merchant Commerce Services, the merchant's customer has one connection and interfaces with the merchant only. CyberSource manages the back-office transaction processing including credit card processing, **fraud** screening and electronic fulfillment. CyberSource electronically interfaces with distributors, clearing houses and fulfillment houses on...

...CyberSource Expertise

CyberSource has developed special technologies, based on the company's extensive experience in **electronic commerce** with

software.net,
that provide the necessary security and protection for distributors,
resellers and publishers implementing **electronic transaction** processing
and distribution via the Internet. These important technologies
include:

CyberSource **Fraud Screen Technology(TM)** which mitigates the **risk**
of **fraudulent** credit card transactions. CyberSource **Fraud Screen**
Technology(TM), based on artificial intelligence software developed by
the company, analyzes each credit card transaction looking for
characteristics that may indicate the transaction is **fraudulent**.

Electronic Distribution Technology (EDT) which provides secure
distribution of digital products by encrypting the content...

...shipping container and launch the install script for the product.
Before the product installs, the **shipping** container self-**checks** to
ensure that the product has not been infected with a virus, or otherwise
corrupted during shipment.

CyberSource Corp.

CyberSource Corp. is a privately held company specializing in
advanced, customized **Internet commerce** services including secure
transaction processing and electronic distribution of software and other
digital products. CyberSource...

20/3,K/32 (Item 14 from file: 813)
DIALOG(R)File 813:PR Newswire
(c) 1999 PR Newswire Association Inc. All rts. reserv.

0943192 LATU045
CYBERSOURCE'S NEW INTERNET COMMERCE SERVICES PROVIDE SOFTWARE
PUBLISHERS TURN-KEY ELECTRONIC TRANSACTION AND DISTRIBUTION
SERVICES

DATE: April 30, 1996 08:05 EDT WORD COUNT: 801

CYBERSOURCE'S NEW INTERNET COMMERCE SERVICES PROVIDE SOFTWARE
PUBLISHERS TURN-KEY ELECTRONIC TRANSACTION AND DISTRIBUTION
SERVICES

, April 30 /PRNewswire/ -- CyberSource Corp., the
leading Internet-based electronic distribution company, announced today
Internet Commerce Services (ICS), a broad range of turn-key services
which provide secure **electronic transaction** processing and distribution
of digital products via the Internet. Companies such as Qualcomm,
Insignia and...

...chosen CyberSource to get their products to
market faster, leveraging CyberSource's secure technology and **electronic**
commerce expertise as an early pioneer of electronic distribution and
founder of software.net.

With services...

...from co-branded Web sites at software.net
to independent customer sites constructed with CyberSource **electronic**
commerce technology, ICS provides publishers with one-stop shopping for
complete back-office **electronic transaction** and distribution services.

"We teamed with CyberSource for our first venture into **electronic commerce** because of the breadth of services they offer and their extensive experience in this area...

...Lee, president and CEO of Insignia Solutions. "So far we are very pleased with our **Internet sales** of MacTransfer for Windows 95. Working with CyberSource has allowed us to bring the product...

...R) Software Corp. to sell Envoy(TM); and ViaSoft International to sell Speed Surfer(TM).

Internet Commerce Services

As a provider of integrated **electronic commerce** services, CyberSource offers:

Real-time credit card transaction processing which completes all the steps in the credit card purchasing process;

Credit card anti- **fraud** technology developed by CyberSource which protects the merchant by analyzing all transactions to reduce the **risk** of **fraud** ;

Electronic fulfillment which provides immediate distribution of products using CyberSource's high speed connectivity;

Secure...

...to government regulations and publisher requirements;

Expert customer support to serve the unique needs of **online** customers;

Sales reports to track daily **electronic sales** activity;
100% customer registration which provides crucial marketing information for database marketing activities.

Fraud protection

A major concern of merchants doing business on the Internet is the danger of **fraudulent** credit card purchases. To protect merchants, CyberSource developed CyberSource **Fraud** Screen Technology(TM) which is based on artificial intelligence software. This technology analyzes each credit card transaction looking for characteristics that may indicate the transaction is **fraudulent** . Every credit card transaction processed by CyberSource is not only validated by the bank in real-time, but also analyzed by the CyberSource **Fraud** Screen Technology to mitigate the **risk** of **fraud** for merchants.

Secure distribution of digital products

CyberSource has developed Electronic Distribution Technology (EDT) which...

...shipping container and launch the install script for the product. Before the product installs, the **shipping** container self- **checks** to ensure that the product has not been infected with a virus or otherwise corrupted during shipment.

CyberSource Corp.

CyberSource Corp. is a privately held company specializing in advanced, customized **Internet commerce** services including secure transaction processing and electronic distribution. CyberSource owns software.net (<http://software.net...>)

20/3,K/33 (Item 1 from file: 634)
DIALOG(R)File 634:San Jose Mercury
(c) 2005 San Jose Mercury News. All rts. reserv.

08628039

BILL SEEKS INTERNET ACCOUNTABILITY FIRST LEGISLATION TO ADDRESS ELECTRONIC CONSUMER FRAUD

San Jose Mercury News (SJ) - Tuesday, May 7, 1996
By: Rebecca Smith, Mercury News Consumer Writer
Edition: Morning Final Section: Front Page: 1A
Word Count: 829

BILL SEEKS INTERNET ACCOUNTABILITY FIRST LEGISLATION TO ADDRESS ELECTRONIC CONSUMER FRAUD

TEXT:

... Francisco, said AB 3320 is a "gentle approach" to the growing problem of electronic consumer **fraud**. It would require all vendors using the Internet to disclose their addresses and refund policies...

... Lungren behind the measure was highly symbolic. Credit card companies, which suffer heavy losses from **fraud**, should be pleased by the bill.

Speier said on-line customers can be **cheated** in one of two ways. A scam artist may obtain an identification number (credit card...

...buy themselves either aren't delivered or turn out to be shoddy.

"The standards for **Internet commerce** should be just as high as for telemarketers or mail order," said Speier, former chairwoman...

... over the Internet. "We can't even get good numbers on Internet users, let alone **fraud**. It's just growing too fast," said Steve Telliano, press secretary for the attorney general...

... able to put people in touch with foundations offering huge cash grants. Another promoted high- **risk** stocks. A third promised a \$24 cure for AIDS.

Coinciding with the news conference was...

...common Internet complaints:

(box) Deceptive marketing practices.

(box) Inaccurate on-line information.

(box) Financial scams, **frauds** and impersonations.

(box) "Spamming" or the distribution of electronic junk mail.

(box) Copyright and trademark...

... Speier urged consumers to visit two Web sites devoted to alerting the public to Internet **fraud**.

(box) The National **Fraud** Information Center tells consumers about Internet scams and gives tips on how to avoid being victimized. Address: <http://www.fraud.org>.

(box) The California Alliance for Consumer Protection maintains a site containing several resources including...

... the Assembly Consumer Protection Committee. Address: <http://www.consumers.com>.

INFOBOX: TIPS TO AVOID CYBERSPACE **FRAUD**

Ten ways to spot an Internet bandit:

1. Hidden name or address. Don't conduct business with anyone who won't give you a **verifiable** name, **address** and telephone number.
2. Impossible to check references. ''As seen on Donahue'' or ''as seen ...''

DESCRIPTORS: CONSUMER **FRAUD** POLITICS COMPUTER INFORMATION
TELECOMMUNICATION COMMUNICATION SERVICE BUSINESS COMPANY
TECHNOLOGY\

Assembly Consumer Protection Committee ; California Alliance for Consumer Protection ; National **Fraud** Information Center ; Social Security